

深空® web 應用防火牆系統

SkyDeep® Web Application Firewall System

Version 1.x 管理員指南

“網站安全深度防禦”

更新日期: 2014-10

最新資訊: <http://www.sky-deep.com>

版權所有© 2014 福州深空®資訊技術有限公司

Copyright© 2014 FuZhou SkyDeep Information Technology Co.,Ltd

目錄

第一章	歡迎使用 “深空 WEB 應用防火牆系統”	- 7 -
第二章	產品術語、部署、原理、安全架構	- 9 -
一、	產品術語	- 9 -
二、	產品部署、原理、安全架構	- 10 -
第三章	快速使用說明	- 11 -
第四章	系統需求、安裝與啟動	- 12 -
一、	系統需求	- 12 -
二、	安裝與啟動	- 13 -
第五章	產品管理概述	- 15 -
一、	選擇用戶端介面語言	- 15 -
二、	連接伺服器	- 15 -
三、	一次同時登錄多台伺服器(批量登錄)	- 16 -
四、	規則運算式測試工具	- 17 -
五、	查看所有網站資訊	- 17 -
六、	創建私有/刪除私有/修改公共或私有 WAF 策略	- 18 -
七、	遮罩所有私有策略	- 19 -
八、	重載所有策略	- 20 -

第六章 WAF 公共/私有策略 操作	- 21 -
一、 WAF 運行模式	- 21 -
二、 IIS 配置保護策略.....	- 22 -
三、 策略作用於 HTTPS.....	- 23 -
四、 WAF 對攔截請求的處理.....	- 23 -
五、 禁止代理訪問策略	- 24 -
六、 IP 存取控制策略(IP 黑/白名單).....	- 24 -
七、 IP 存取控制策略(IP 動態白名單).....	- 26 -
八、 特權 IP 策略.....	- 27 -
九、 主動防禦策略(IP 訪問行為監視)	- 27 -
十、 主動防禦策略(URL 訪問次數限制)	- 28 -
十一、 防盜鏈策略	- 29 -
十二、 HTTP 策略(通用頭部)	- 29 -
十三、 HTTP 策略(請求頭部)	- 30 -
十四、 HTTP 策略(實體頭部)	- 30 -
十五、 HTTP 策略(用戶自訂頭部)	- 31 -
十六、 HTTP 策略(返回頭部)	- 31 -
十七、 HTTP 策略(請求方式)	- 32 -
十八、 HTTP 策略(限制頭部總長)	- 33 -
十九、 URL 策略(URL 最大長度)	- 34 -
二十、 URL 策略(URL 參數部分最大長度)	- 34 -
二十一、 URL 策略(URL 非參數部分最大長度)	- 34 -

二十二、	URL 策略(URL 非參數部分關鍵字過濾)	- 35 -
二十三、	URL 策略(URL 參數部分關鍵字過濾)	- 35 -
二十四、	URL 策略(URL 參數部分關鍵字過濾-白名單策略).....	- 37 -
二十五、	URL 策略(URL 參數部分關鍵字過濾-黑名單策略).....	- 40 -
二十六、	URL 策略(URL 黑名單)	- 40 -
二十七、	URL 策略(特權 URL)	- 41 -
二十八、	URL 策略(URL+IP 限制).....	- 41 -
二十九、	URL 策略(URL 請求檔案類型限制)	- 42 -
三十、	POST 策略(POST 請求內容關鍵字過濾)	- 42 -
三十一、	POST 策略(POST 請求 URL 限制)	- 43 -
三十二、	COOKIE 策略(COOKIE 內容關鍵字過濾).....	- 44 -
三十三、	IIS 返回資料策略(HTTP 返回狀態碼過濾).....	- 45 -
三十四、	IIS 返回資料策略(HTTP 返回內容過濾/網頁內容過濾)	- 48 -
三十五、	頻寬策略	- 49 -
三十六、	動態特權 IP 策略	- 50 -
第七章	製作硬體 WAF	- 54 -
一、	硬體準備	- 55 -
二、	軟體準備	- 55 -
三、	部署方式	- 56 -
四、	其它選項說明	- 59 -
第八章	日誌類操作	- 61 -

一、	查看日誌檔內容	- 62 -
二、	日誌檔管理	- 63 -
三、	日誌記錄物件管理	- 63 -
第九章 產品系統操作		- 65 -
一、	產品用戶端登錄 IP 限制	- 65 -
二、	產品服務端綁定 IP/埠	- 66 -
三、	系統控制	- 66 -
四、	產品預設行為	- 66 -
五、	用戶管理	- 67 -
六、	文件管理	- 68 -
七、	命令列	- 69 -
第十章 不同環境下的注意事項		- 70 -
一、	WINDOWS XP x64 / WINDOWS SERVER 2003 x64 作業系統	- 70 -
二、	IIS7.0 及其以後版本的環境中	- 72 -
三、	VISTA/2008 及以後的 x64 作業系統	- 74 -
四、	網域控制站 (DOMAIN CONTROLLER) 上的額外操作	- 76 -
第十一章 使用審計策略		- 80 -
一、	啟用對象訪問審計策略	- 80 -
二、	查看物件訪問審計日誌	- 81 -
第十二章 卸載產品		- 83 -

一、 卸載前的注意事項	- 83 -
二、 打開卸載程式	- 83 -
三、 開始卸載	- 83 -
第十三章 技術支援及聯繫方式	- 84 -

第一章 歡迎使用

“深空 web 應用防火牆系統”

“深空 web 應用防火牆系統”是由 福州深空資訊技術有限公司 自主研發而成的,具有完全自主智慧財產權的 Web 應用防火牆軟體產品.

在防禦 web 攻擊安全性原則上,本產品含有: IIS 配置保護、禁止代理訪問、IP 存取控制(黑名單、白名單、動態白名單(抗應用層 CC 攻擊,應用層 DDOS 攻擊,機器人訪問等)、特權 IP)、IP 訪問行為主動防禦(抗應用層 CC 攻擊,應用層 DDOS 攻擊)、URL 訪問次數主動防禦(抗應用層 CC 攻擊,應用層 DDOS 攻擊)、防盜鏈、HTTP 通用頭部各成員長度檢查、HTTP 請求頭部各成員長度檢查、HTTP 實體頭部各成員長度檢查、HTTP 用戶自訂頭部各成員長度檢查、HTTP 返回頭部各成員內容過濾、HTTP 請求方式限制、HTTP 頭部總長檢查、URL 總長限制、URL 參數部分長度限制、URL 非參數部分長度限制、URL 非參數部分關鍵字過濾、URL 參數部分關鍵字過濾(白名單策略、黑名單策略、自訂放行關鍵字和自訂強制攔截關鍵字)、URL 黑名單檢查、特權 URL 檢查、URL+IP 存取控制、URL 請求檔案類型檢查、POST 請求內容過濾、POST 請求的 URL 限制、COOKIE 內容關鍵字過濾、HTTP 返回狀態碼過濾、HTTP 返回例外狀態碼設置、HTTP 返回內容過濾(網頁內容過濾)、各網站目錄每 IP 最大頻寬限制、IP 動態特權 IP、轉發(反向代理)等 30 多種安全性原則功能.

在管理上,本產品採用 C/S 架構(Client/Server,用戶端/服務端)模式,使用者可以通過用戶端遠端系統管理服務端,功能上有: 查看/修改/啟用/禁用上述安全性原則、限制用戶端登錄的 IP 策略(IP 白名單策略/IP 黑名單策略)、查看/修改產品預設參數(如綁定的 IP,監聽的埠,不同情形下 WAF 的相應形式等)、系統控制(重啟 IIS、關閉 IIS、重啟伺服器、關閉伺服器)、管理員用戶添加/刪除/修改/啟動/禁用、普通用戶添加/刪除/修改/啟動/禁用/許可權設置(本產品的普通使用者這一概念可以方便 IDC 使用者開設 **Web 防火牆網路安全增值服務**)、產品日誌/**Web 防火牆攔截日誌**/管理日誌/錯誤日誌 的 查看/刪除/下載、日誌記錄物件管理(可以只記錄指定策略的攔截日誌)、伺服器檔管理(查看/刪除檔或資料夾(可批量操作)/新建資料夾/重命名檔或資料夾/上傳檔或資料夾(可批量操作)/下載檔案或資料夾(可批量操作))、命令列模擬(遠端模擬執行 **cmd** 命令)等功能.

本產品研製過程中,研發人員與安全研究人員攜手,從入侵的角度思慮駭客可能的攻擊手法,繼而在產品的安全性原則中加以攔截限制,提高產品對駭客的“免疫”程度.

本產品研製過程中,研發人員根據網站管理人員對“低管理開銷、運行維護價值顯性化”的需求,提供了諸如遠端策略管理、伺服器文件管理、命令列模擬等一系列便利管理功能,充分確保安全與運行維護的高效果和高效率.

“深空 web 應用防火牆系統”提供的業界領先的 **Web** 應用攻擊防護能力,保證了使用者 **Web** 應用系統的連續性與高可靠性,有效地降低了安全風險.

第二章 產品術語、部署、原理、安全架構

一、 產品術語

WAF: Web 應用防火牆(Web Application Firewall),如無特別說明,本指南中特指本 Web 應用防火牆產品.

產品服務端: 指安裝完產品後,伺服器中的 WAFSvc.exe 進程,簡稱**服務端**.

產品用戶端: 指 WAF-Client.exe 用戶端介面程式,簡稱**用戶端**.該程式一般運行于管理員 pc 機中,然後進行遠端系統管理產品運行.
出於安全考慮,本產品用戶端有“**管理員用戶端**”和“**普通用戶用戶端**”這兩種.

公共策略: 這是默認策略,有且僅有一個,默認所有網站都使用公共策略.

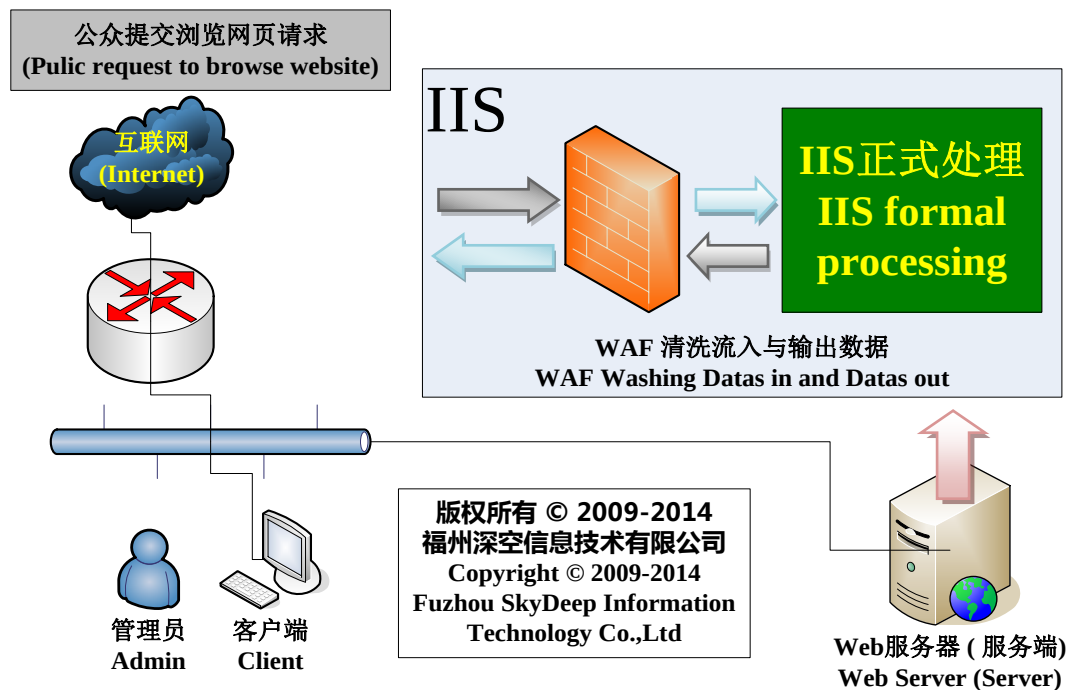
私有策略: 可以有多個,使用者對某個網站配置獨立的防護策略,這一策略即為私有策略.使用私有策略的網站,其防護策略不受公共策略的影響,除非 **WAF** 配置成“**遮罩私有策略**”.

遮罩私有策略: **WAF** 將忽略所有的私有策略,強制所有網站都使用公共策略.

產品管理員: 對產品具有完全控制許可權的用戶,簡稱 **管理員** .

普通用戶: 只能管理部分私有策略的低許可權用戶.

二、 產品部署、原理、安全架構



上圖所示:

服務端安裝在 web 伺服器中,使用者通過用戶端可以遠端系統管理服務端.

服務端在 IIS 中內置安全檢測模組,對所有的流入與流出請求作出分析,再裁定是否放行或採取相關動作,這一過程好比“清洗流入與流出 IIS 的資料”。

第三章 快速使用說明

提示:使用者可直接觀看隨本指南一起分發的相關演示視頻而無需閱讀後文

注意:如果本產品安裝在 64 位元作業系統上,或者安裝在 IIS7.0 及其以後版本的系統中時,或者安裝在網域控制站 (Domain Controller) 上,在安裝產品前,[須進行一些額外配置](#).

第一步:停止 IIS 的運行 (iisreset /stop) ;

第二步:安裝**服務端**程式 WAF-Setup.exe,隨後按提示操作,直至安裝完成;

第三步:重新開啟 IIS 的運行(iisreset /start) ;

打開**用戶端**,輸入伺服器的 IP、產品預設的用戶名(admin)、產品預設的密碼 (admin-12345) 連接服務端,開始管理.

完畢.

注意,本產品預設在伺服器上開啟 20011 埠,如果使用者有防火牆,需要開放此埠才能進行遠端系統管理,否則只能進行本地管理(伺服器上打開**用戶端**連接 127.0.0.1).

如果用戶在操作過程中遇到困難,請查閱[技術支援及聯繫方式](#).

第四章 系統需求、安裝與啟動

一、 系統需求

1.電腦硬體性能需求：

處理器： Intel Pentium III 以上

記憶體： 128MB 以上

硬碟： 剩餘空間在 100MB 以上

2.作業系統需求(32 位元/64 位)

Windows 2000

Windows XP Professional

Windows Server 2003

Windows Vista Ultimate

Windows Server 2008

Windows 7 Ultimate

Windows Server 2008 R2

Windows 8

Windows Server 2012

Windows 8.1

Windows Server 2012 R2

使用虛擬化技術後繼續支持下列平臺(32 位/64 位):

Asianux	CentOS
Debian GNU/Linux	Fedora
FreeBSD	Java Desktop System
Mandrake Linux	NetWare
openSUSE	Oracle Enterprise Linux 5
Oracle Linux	Red Hat Enterprise Linux
Red Hat Linux	Solaris
SUSE Linux	SUSE Linux Desktop
SUSE Linux Enterprise	Turbolinux
Ubuntu	

二、 安裝與啟動

注意:如果本產品安裝在 64 位元作業系統上,或者安裝在網域控制站 (Domain Controller) 上,在安裝產品前,[須進行一些額外配置](#).

第一步:將產品安裝光碟放入光碟機中,然後按兩下光碟根目錄下的產品安裝程式 **WAF-Setup.exe**,仔細閱讀彈出對話方塊中的”使用者授權合約”,如果不同意該協議,則點擊”不同意/退出(**Exit**)”退出安裝.如果同意該協議,則勾選“我

已認真閱讀並同意上述協議” ,然後點擊” 同意/下一步(Next)” ,繼續後面的步驟.

第二步:停止 IIS 的運行,選擇安裝目錄,然後點擊” 開始安裝 (Install)” ,隨後等待安裝完成即可關閉視窗,如下圖所示:



第三步:開啟 IIS 的運行.

第五章 產品管理概述

一、 選擇用戶端介面語言

使用者可根據自身情形,選擇適合自己的用戶端介面語言.操作方法是:打開用戶端,關閉登錄框,然後在用戶端視窗的標題列中點擊右鍵,即可選擇用戶端語言.

如下圖所示:



選擇新的語言後,重新打開用戶端即可生效.

二、 連接伺服器

打開用戶端,連接伺服器,輸入相關資訊(預設使用者名:admin,預設密碼:admin-12345):



注意:第一次登錄後,請立即在”產品系統”->”使用者管理”中修改預設使用者名和預設密碼.

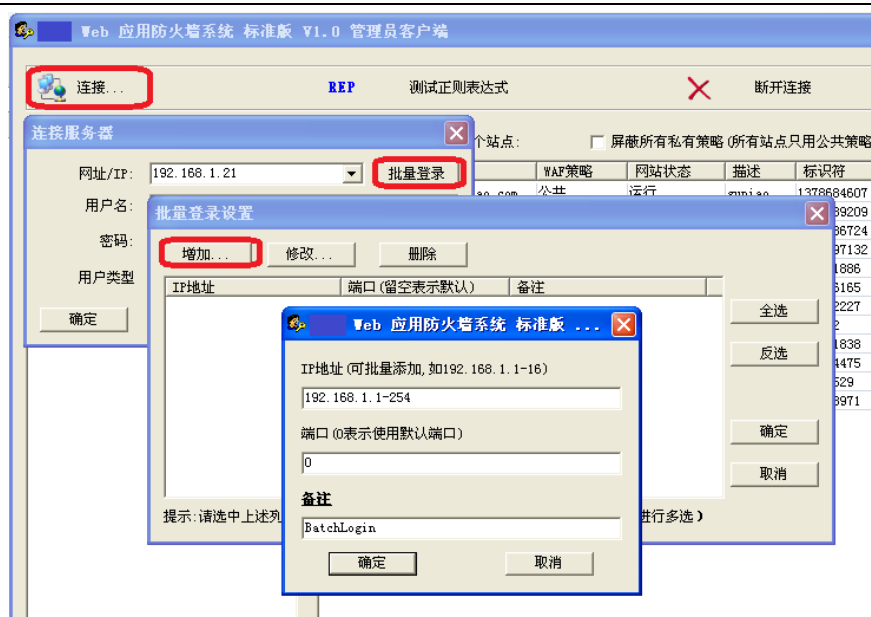
提示:本產品用戶端和服務端之間的通信已經加密,而且在用戶端登錄時使用 **NTLM** 技術進行認證,因而可以防止協力廠商從網路中嗅探密碼。

登錄後可以看到類似如下圖所示的管理介面,左邊為**樹形清單區**,右邊為**資訊顯示區**。



三、 一次同時登錄多台伺服器(批量登錄)

用戶可以同時連接其它單個伺服器,也可以使用批量登錄,一次同時連接多達 254 個伺服器,如下圖所示:



四、規則運算式測試工具

用戶端提供了測試規則運算式的簡易工具,在工具列中點擊“測試規則運算式”,用戶可以輸入規則運算式和測試文本來調試規則運算式,如下圖所示:



注:本產品中使用的規則運算式遵從 **Visual Basic** 規則運算式語法.

五、查看所有網站資訊

資訊顯示區中,使用者可以看到當前伺服器上的所有網站的相關資訊,包括:

網站總數、網站運行狀態、網站名稱、網站根目錄、綁定的 IP 地址、網站綁定的埠、網站對應的功能變數名稱、網站識別字、WAF 策略、HTTPS 埠等資訊。

六、 創建私有/刪除私有/修改公共或私有 WAF 策略

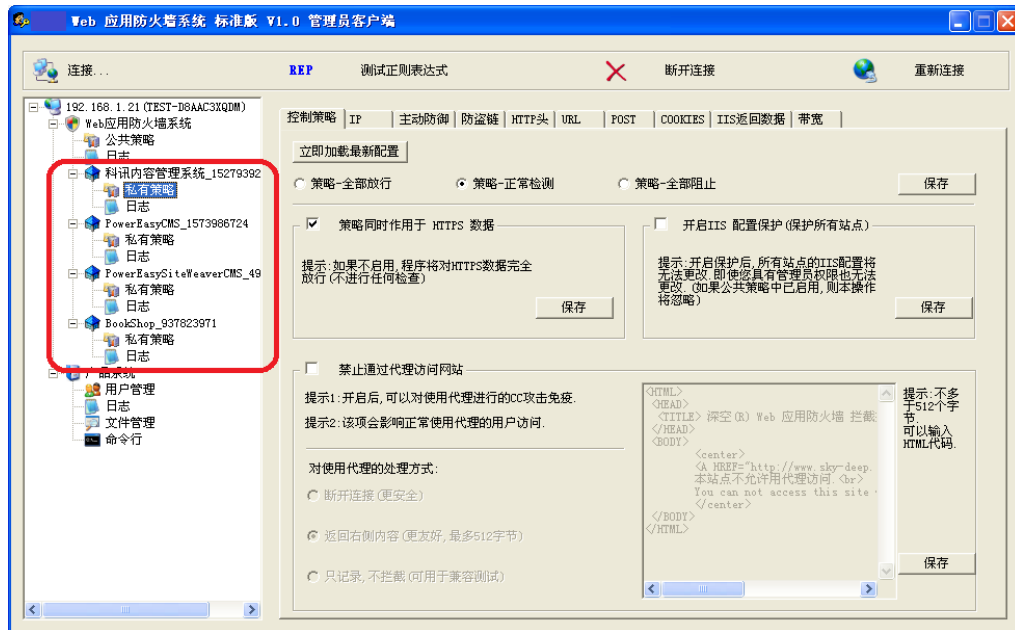
普通的 Web 應用防火牆,如論是軟體還是硬體,其策略都是只能作用於所有的網站,如果某台伺服器中含有大量的不同類型的網站,則用一種攔截策略去防禦所有類型的網站就經常會遇到相容性嚴重下降等問題。

例如,假設某台伺服器上有 `www.123.com` 和 `www.456.com` 這兩個網站,其中,前者的網站在 URL 參數部分中需要攔截 “--” 等 SQL 注入關鍵字,而後者的網站它本身正常的 URL 參數部分中就含有 “--” 關鍵字。這時,如果策略中攔截了 “--” 關鍵字就勢必影響後者的網站正常工作,而如果不攔截 “--” 關鍵字,則前者的網站就很有可能暴露於 SQL 注入的危險之中。

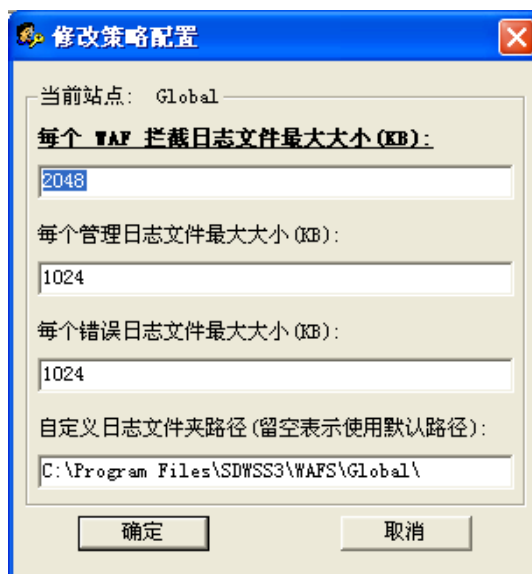
使用者通過使用本產品的“私有策略”這一新概念,可以對此情形應付自如。

資訊顯示區中,管理員使用者通過“使用私有策略”/“刪除”按鈕,可以給單個網站設置 使用/刪除 獨立的 WAF 策略(私有策略)。這樣設置後,該網站將使用自己獨立的 WAF 策略(私有策略),不受公共策略(除非管理員用戶開啟了“遮罩所有私有策略”)和其它私有策略的影響。

如下圖所示創建了 4 個私有策略,每一個私有策略都對應一個網站:



資訊顯示區中,使用者通過“修改”按鈕,可以設置公共策略/私有策略的各類日誌檔單個最大大小和日誌資料夾路徑,如下圖所示。



提示:根據版本的不同(如企業版,標準版,高級版等),用戶可創建的最多私有策略的個數也不同。

七、遮罩所有私有策略

資訊顯示區中,使用者通過“遮罩所有私有策略”按鈕,可以使得 WAF 忽略

所有的私有策略,強制所有網站使用公共策略.

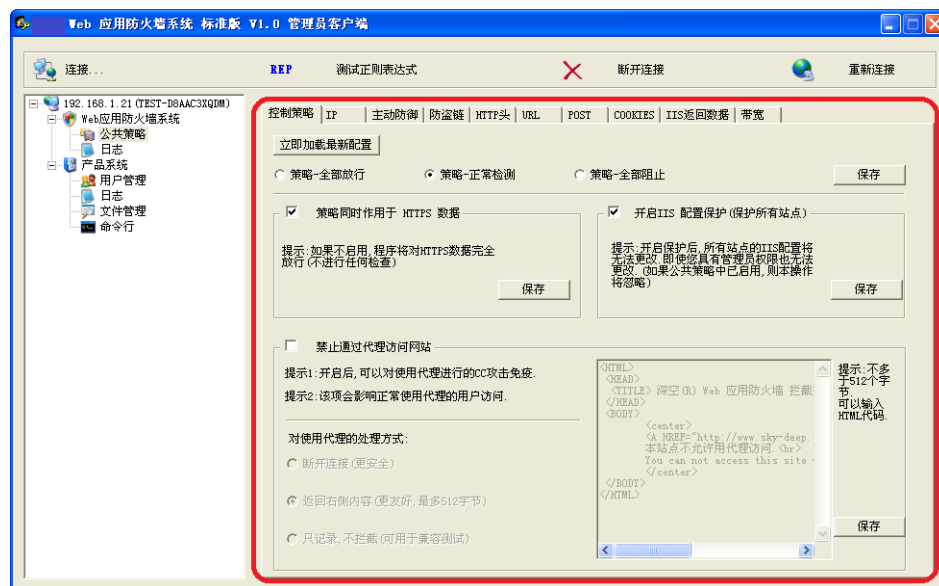
注意:此功能需點擊“重載所有策略”後方能生效.

八、 重載所有策略

資訊顯示區中,使用者通過“重載所有策略”按鈕,可以使 **WAF** 立即重新載入公共策略和所有的私有策略.

第六章 WAF 公共/私有策略 操作

本章介紹的是 產品用戶端->左邊樹形清單->Web 應用防火牆系統->公共/私有策略 的操作,各子策略對應的介面在右邊的資訊顯示區中。



使用者亦可觀看隨本指南一起分發的相關演示視頻而無需閱讀後文。

商業版用戶如果在操作中遇到困難,可以[查看最後一章以尋求技術支援](#)。

一、 WAF 運行模式

本產品提供了如下三種 WAF 的運行模式:

- 策略-全部放行:** WAF 放行所有請求,不進行任何安全檢測。
- 策略-正常檢測:** WAF 根據使用者配置的相關安全性原則,對流入與流出 IIS 的資料進行正常檢測與清洗。
- 策略-全部阻止:** WAF 阻止所有的請求。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

二、 IIS 配置保護策略

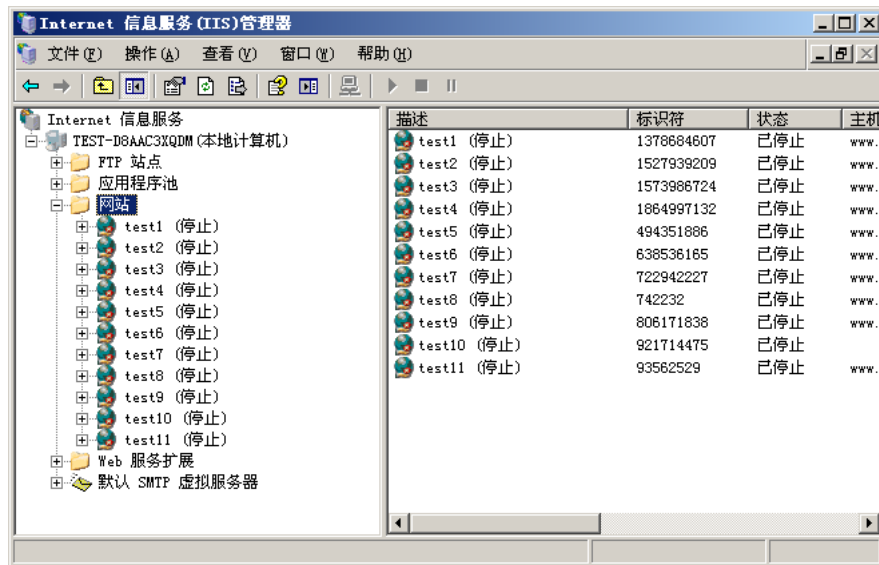
本產品提供的 IIS 配置保護功能實現了對 IIS 配置資料的防篡改,啟用保護後,受保護網站的 IIS 配置資料(如,網站名稱、網站根目錄、預設首頁文檔、應用程式池、篩選器清單等)將無法被篡改,即使惡意使用者具有作業系統管理員許可權.

下圖顯示了在“公共策略”中開啟了“IIS 配置保護”後,以作業系統的 Administrators 組成員的身份打開 inetmgr.msc,即 Internet 資訊服務(IIS)管理器,然後任選一個網站,查看其 屬性 資訊的情形.從圖中可以發現,相關屬性都已經灰化而不可更改.



提示:如果在“公共策略”中開啟了“IIS 配置保護”,則 IIS 中所有網站的配置都同時得到了保護.如果在某個“私有策略”中開啟了“IIS 配置保護”,則只有這個私有策略對應網站的 IIS 配置才能防篡改.

注意:開啟“IIS 配置保護”後,網站正常運行將不受影響,但 IIS 將無法正常更新網站狀態資訊,因此使用者在 IIS 管理器中查看網站狀態時,將可能看到類似如下圖所示資訊,雖然此時網站實際是正常運行:



警示：當使用者卸載產品前,使用者應該確保公共策略和各私有策略中的 IIS 配置保護已取消,否則產品卸載後,使用者依然會無法更改網站的 IIS 配置資訊。

三、 策略作用於 HTTPS

本產品可以供使用者選擇是否對 HTTPS(Secure Hypertext Transfer Protocol),即安全超文字傳輸協定 的資料進行安全檢測。

警示：如果不開啟,則 WAF 對 HTTPS 類的資料全部放行。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

四、 WAF 對攔截請求的處理

WAF 對攔截請求的處理,使用者有三種處理方式可以選擇:

- 斷開連接(更安全):** 立即斷開連接。
- 向流覽者發送指定資訊:** 比如向流覽者發送“拒絕訪問”等文字。
- 只記錄,不攔截(可用於相容測試):** WAF 記錄下所有不合策略的請求但不攔截.本方式可以用來測試當前策略和網站的相容程度,這期間網站的

正常運行不受影響,用戶可以逐步調試策略,直至滿意為止.

五、 禁止代理訪問策略

如果開啟本策略,WAF 將對通過代理訪問的流覽請求進行攔截.

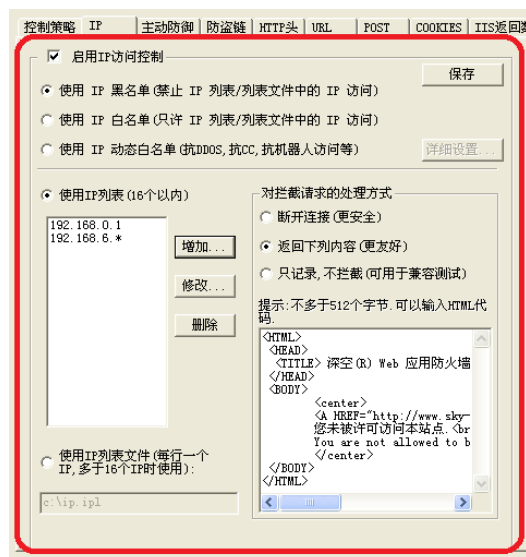
保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

六、 IP 存取控制策略(IP 黑/白名單)

如果開啟本策略,而且選擇 **IP 黑名單** 策略,則 WAF 將對黑名單中的 IP 進行遮罩,被遮罩的 IP 將無法訪問任何頁面.

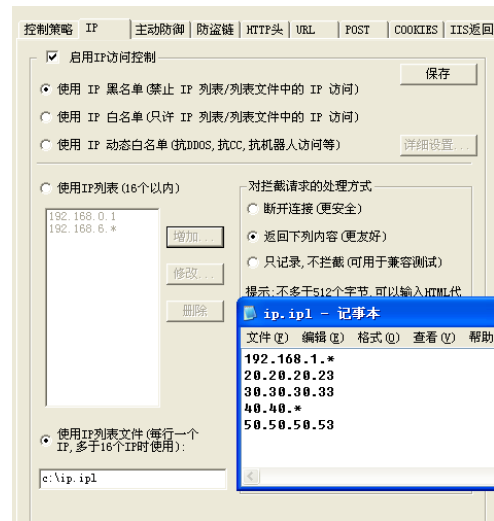
如果開啟本策略,而且選擇 **IP 白名單** 策略,則 WAF 將只允許白名單中的 IP 訪問,非白名單 IP 都將被遮罩,被遮罩的 IP 將無法訪問任何頁面.

如果黑/白名單 IP 的個數不超過 16 個,則用戶可以在用戶端中設置具體的 IP,可以使用星號萬用字元,如下圖所示:



如果黑/白名單 IP 的個數超過 16 個,則必須使用 IP 列表檔,並在用戶端中配置 IP 清單檔的全路徑.IP 清單檔中每一行配置一個 IP,可以使用星號萬用字元,如

下圖所示:



提示:IP 列表檔的拓展名必須是 .ipl

提示:如果用戶具有網站合法流覽者的 IP 地址清單,並把這些 IP 位址寫入 IP 列表檔中(如果合法者 IP 超過 16 個時),然後使用這裡提及的 IP 存取控制白名單策略,則可以極大地提升網站的安全性.

警示：用戶必須確保黑/白名單 IP 列表檔存在,而且拓展名為.ipl,否則將無法保存配置,或者 WAF 將無法正常運行.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

七、 IP 存取控制策略(IP 動態白名單)

IP 动态白名单

IP动态白名单 (抗DDOS, 抗CC, 抗机器人访问等):
提示: 用户可以参考管理员/用户指南了解详细原理与用法.

非白名单中的 IP 访问控制

非白名单中的IP允许访问的URL (及其子URL)
作用: 使非白名单中的 IP 有机会通过访问本设置中的 URL 而成为白名单中的 IP

/Dynamic_White_IP/asp/

把非白名单 IP 的请求重定向到下面的 URL .

/Dynamic_White_IP/asp/default.asp

保存

白名单 IP 文件 (拓展名必须是 .ipl)

白名单 IP 文件全路径 (注意: 文件必须存在):

C:\Web\Dynamic_White_IP\asp\IP.ipl

每隔 3 秒读取一次白名单 IP 文件 (最小值为3)

每隔 600 分钟清空一次白名单 IP 文件 (最小值为1)

保存

如果開啟本策略,而且選擇**IP 動態白名單**策略,則受保護網站將具備**抵禦應用層 CC 攻擊**,**抵禦應用層 DDOS 攻擊**,**抵禦機器人訪問**,**防盜鏈**等能力.

IP 動態白名單是 WAF 和網站應用互動的一種模式.此時,WAF 使用 IP 白名單策略,初始時 IP 白名單列表為空,隨後 WAF 每隔一定時間(如每隔 3 秒)讀取指定 IP 列表檔中的 IP 並更新到 IP 白名單列表中.

使用者可以在網站中設置一個驗證頁面(如 /Dynamic_White_IP/asp/default.asp),把經過驗證的(比如:能正確輸入驗證碼的/能正確回答問題的 等)IP 寫入指定檔中(每行一個 IP),如: C:\Web\ Dynamic_White_IP\asp\IP.ipl .然後 WAF 每隔一定時間(如每隔 3 秒)讀取一次這個 IP.ipl 檔,並更新到 WAF 內部的 IP 白名單列表中,隨後這個經過驗證的 IP 就可以正常流覽網站.

對任意一個未經驗證的 IP(WAF 內部的 IP 白名單清單中無此 IP 記錄),無論訪問任何頁面,都會被自動重定向到驗證頁面中(如 /Dynamic_White_IP/asp/default.asp).

ault.asp).

對已經經過驗證的 IP(WAF 內部的 IP 白名單清單中存在此 IP 記錄),其可正常流覽網站,不再受本策略限制.

警示:使用者必須確保動態白名單 IP 清單檔存在,而且拓展名為.ipl,否則將無法保存配置,或者 WAF 將無法正常運行.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

八、特權 IP 策略

如果開啟本策略,則特權 IP 列表中的 IP 將不受任何 WAF 策略限制.WAF 將對特權 IP 的流入/流出資料完全放行.

警示:由於特權 IP 不受任何 WAF 策略限制,所以用戶應對特權 IP 列表中的成員進行嚴格審核.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

九、主動防禦策略(IP 訪問行為監視)

The screenshot displays the 'Active Defense' configuration page for 'IP Access Behavior Monitoring'. The page includes several tabs at the top: 'Control Strategy', 'IP', 'Active Defense', 'Anti-DDoS', 'HTTP Header', 'URL', 'POST', 'COOKIES', 'IIS Return Data', and 'Bandwidth'. The 'IP' tab is currently selected.

Under the 'Active Defense-IP Access Behavior Monitoring' section, there are several configuration options:

- ☒ **启用策略:** 满足下面条件时,在指定时长内禁止源IP访问. (Save button)
- 对违规的 IP 在:** 600 秒内禁止其访问
- ☒ **对同一IP地址:** 10 秒内访问不存在的页面 20 次以上时,禁止源IP访问.
- ☐ IIS 处理前,进行检测 ☐ 推荐: IIS处理后,返回给用户之前,进行检测
- ☒ **对同一IP地址:** 3 秒内请求 48 次以上时,禁止源IP访问.
- 对拦截请求的处理方式:**
 - ☐ 断开连接(更安全)
 - ☒ 返回下列内容(更友好)
 - ☐ 只记录,不拦截(可用于兼容测试)

The 'Return the following content' option is selected, and the content is displayed in a text area:

```
<HTML>
<HEAD>
<TITLE> 深空(R) Web 应用防火墙 拦截提示</TITLE>
</HEAD>
<BODY>
<center>
<A HREF="http://www.sky-deep.com">B>深空
Web 应用防火墙</A></A> 拦截提示<br><br>
IP行为异常:您的IP已被列入临时黑名单.<br>
Your IP is in black ip list
temporary.<br>
</center>
</BODY>
</HTML>
```

A提示:不多于512个字节,可以输入HTML代码.

如果開啟本策略,WAF 可以對每一個 IP 的訪問行為進行監視與統計,因而受保護網站將具備一定的抵禦應用層 CC 攻擊,抵禦應用層 DDOS 攻擊,抵禦機器人訪問等能力.

本策略具體分為訪問頻率監視和訪問不存在頁面的頻率監視這兩種.

由於駭客攻擊網站時,通常會使用各種 web 漏洞掃描軟體對網站進行快速的掃描,如 SQL 注入工具頻繁對某一頁面或多個頁面進行快速地 SQL 注入請求,網站檔刺探工具每秒嘗試猜測數十個甚至上百個不存在的頁面 等.

因此,通過訪問頻率監視和訪問不存在頁面的頻率監視,WAF 能夠對各類惡意掃描 IP 進行事前主動攔截防禦--在指定時間內遮罩該 IP 的訪問.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

十、 主動防禦策略(URL 訪問次數限制)



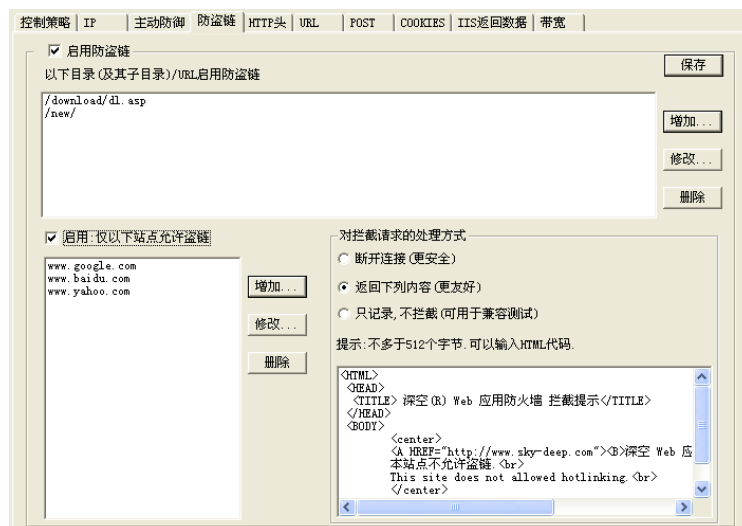
如果開啟本策略,WAF 可以監視與限制指定 URL 每秒最大被請求的次數,因而受保護網站將具備一定的抵禦應用層 CC 攻擊,抵禦應用層 DDOS 攻擊,抵禦機器人訪問等能力.

例如在 CC 攻擊中,攻擊者會對網站中執行時間較長的頁面(如論壇網站中的資料查詢頁面等)進行頻繁地請求,據此不斷消耗伺服器的資源,最終造成網站無法正常工作。

通過設置 URL 訪問次數限制,WAF 將確保受限制的 URL 每秒最多只有指定次數的請求,超出的部分都將被遮罩。例如對某頁面限制每秒最多有 10 次的請求,則在一秒內,前 10 次的請求都不攔截,第 11 次以後的請求都將被遮罩。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

十一、防盜鏈策略

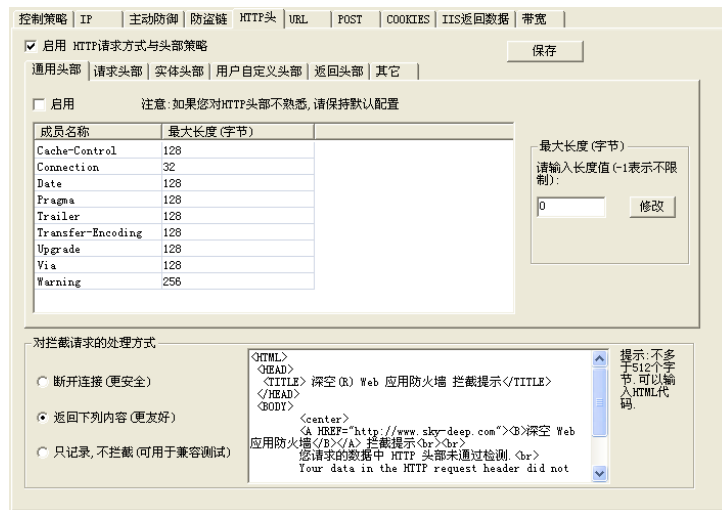


如果開啟本策略,WAF 將對指定 URL 的請求進行檢測是否是盜鏈。同時,用戶還可以設置允許盜鏈的網站,如各類搜尋引擎,友情網站等。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

十二、HTTP 策略(通用頭部)

提示:如果使用者對 HTTP 協議不熟悉,請保留預設配置。



如果開啟本策略,WAF 將對 HTTP 通用頭部 的各成員長度進行檢查,如有某成員長度超出限制的最大值,則立即對請求進行攔截。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

十三、 HTTP 策略(請求頭部)

提示:如果使用者對 HTTP 協議不熟悉,請保留預設配置。

如果開啟本策略,WAF 將對 HTTP 請求頭部 的各成員長度進行檢查,如有某成員長度超出限制的最大值,則立即對請求進行攔截。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

十四、 HTTP 策略(實體頭部)

提示:如果使用者對 HTTP 協議不熟悉,請保留預設配置。

如果開啟本策略,WAF 將對 HTTP 實體頭部 的各成員長度進行檢查,如有某成員長度超出限制的最大值,則立即對請求進行攔截。

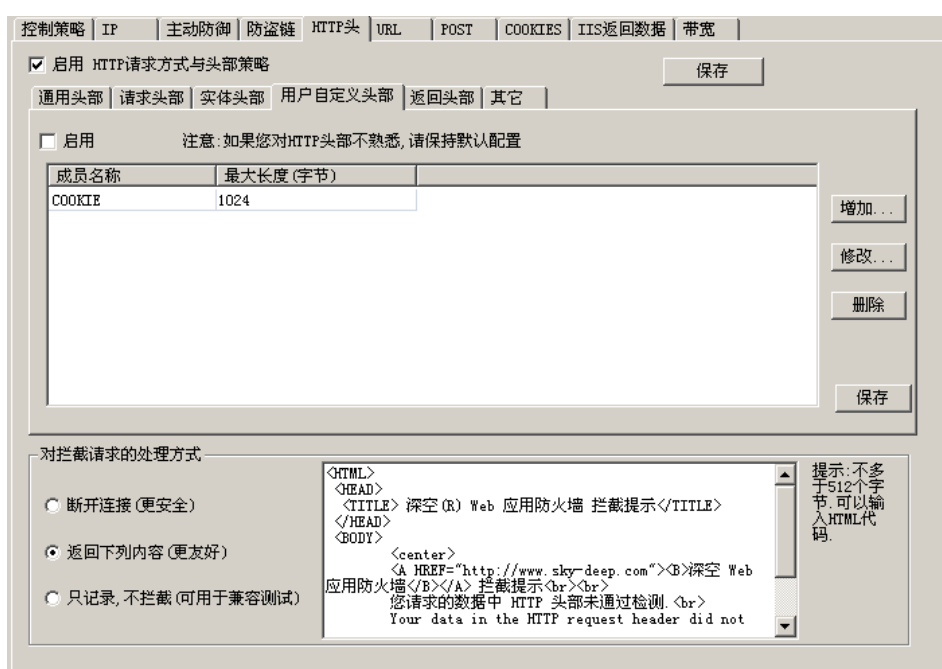
保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

十五、HTTP 策略(用戶自訂頭部)

提示:如果使用者對 HTTP 協議不熟悉,請保留預設配置.

如果開啟本策略,WAF 將對 HTTP 用戶自訂頭部的各成員長度進行檢查,如有某成員長度超出限制的最大值,則立即對請求進行攔截.

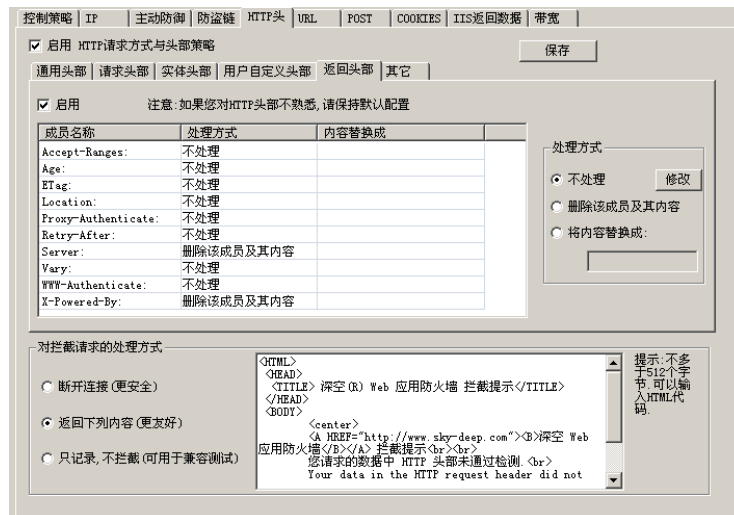
在使用者自訂頭部中,使用者可以自訂增加需要限制最大長度的成員名稱及其限定值,如下圖所示增加限制 COOKIE 成員的最大長度為 1024 個位元組:



保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

十六、HTTP 策略(返回頭部)

提示:如果使用者對 HTTP 協議不熟悉,請保留預設配置.



如果開啟本策略,WAF 將對 HTTP 返回頭部的各成員長度進行安全過濾,如替換其內容/刪除成員及其內容等。

通常,在返回頭部中,一般會洩漏伺服器的一些敏感資訊,這些敏感資訊可被駭客利用來識別伺服器的作業系統和 Web 服務軟體。

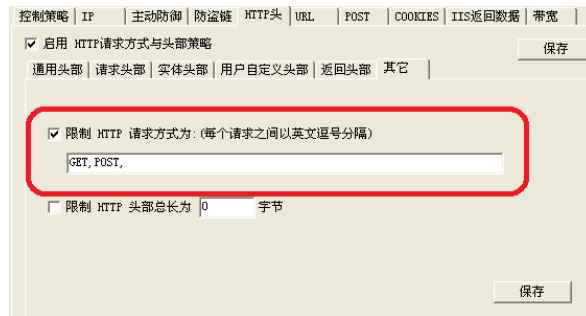
因此,WAF 過濾一些敏感成員,如 Server 成員、X-Powered-By 成員的內容,將增加駭客收集伺服器資訊的難度。

用戶可以在此設置對各返回頭部成員的處理方式,如:刪除成員及內容,替換返回內容等。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

十七、HTTP 策略(請求方式)

提示:如果使用者對 HTTP 協議不熟悉,請保留預設配置。



如果開啟本策略,WAF 將對 HTTP 請求方式 進行檢查,只允許使用者設置的請求方式,其它一律進行攔截.

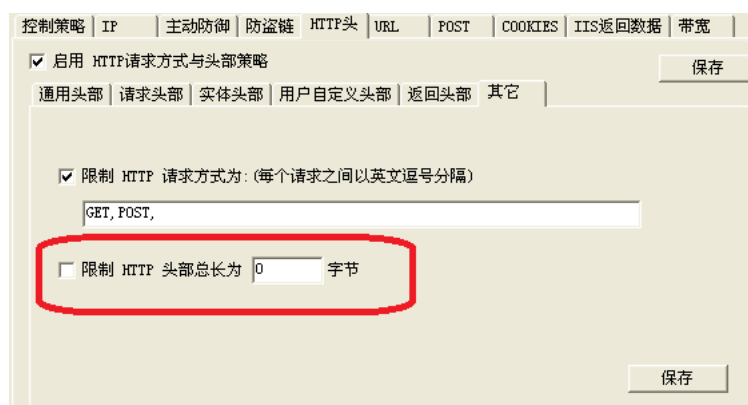
HTTP 請求方式 如 GET,POST,HEAD,OPTION,DELETE,PUT 等,標記了一個 HTTP 請求的在對應的 URL 上所執行的方式,其中 PUT 和 DELETE 是兩個對伺服器比較危險的請求方式.

提示:根據 RFC2616 文檔,請求方式是大小寫敏感的,通常都為大寫.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

十八、 HTTP 策略(限制頭部總長)

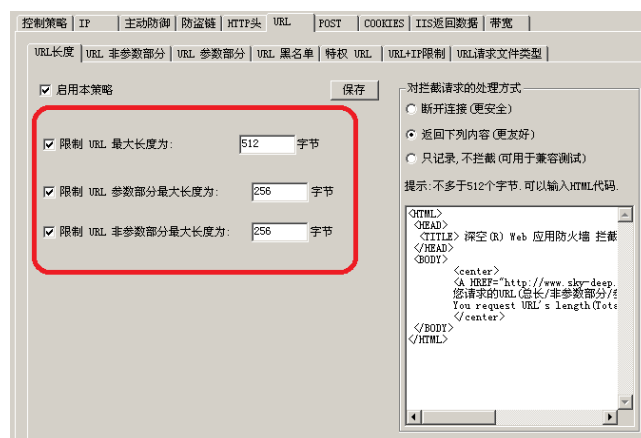
提示:如果使用者對 HTTP 協議不熟悉,請保留預設配置.



如果開啟本策略,WAF 將對 HTTP 頭部總長 進行限制,如果 HTTP 頭部總長超過限制,則 WAF 將對請求進行攔截.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

十九、 URL 策略(URL 最大長度)



如果開啟本策略,WAF 將對 URL 總長進行限制,如果 URL 總長超過限制,則 WAF 將對請求進行攔截。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

二十、 URL 策略(URL 參數部分最大長度)

URL 參數部分是指 URL 中第一個問號後的全部內容,例如 URL:

`/news/news.asp?id=100&update=2011`

URL 參數部分為上面的紅色部分。

如果開啟本策略,WAF 將對 URL 參數部分的長度進行限制,如果 URL 參數部分的長度超過限制,則 WAF 將對請求進行攔截。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

二十一、 URL 策略(URL 非參數部分最大長度)

URL 非參數部分是指 URL 中第一個問號前的全部內容,例如 URL:

`/news/news.asp?id=100&update=2011`

URL 非參數部分為上面的紅色部分.

如果開啟本策略,WAF 將對 URL 非參數部分的長度進行限制,如果 URL 非參數部分的長度超過限制,則 WAF 將對請求進行攔截.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

二十二、 URL 策略(URL 非參數部分關鍵字過濾)

URL 非參數部分是指 URL 中第一個問號前的全部內容,例如 URL:

/news/news.asp?id=100&update=2011

URL 非參數部分為上面的紅色部分.

如果開啟本策略,WAF 將對 URL 非參數部分進行關鍵字過濾.

提示:本產品自帶的 URL 非參數部分關鍵字,將能使 WAF 對利用 IIS 檔拓展名等漏洞進行攻擊的請求進行攔截.

用戶可以設置原始匹配關鍵字(每個關鍵字最長 16 位元組)和規則運算式匹配關鍵字(每個關鍵字最長 64 位元組)這兩種,且都不區分大小寫,WAF 檢測關鍵字時,將分別檢測原始匹配的關鍵字和規則運算式匹配的關鍵字.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

二十三、 URL 策略(URL 參數部分關鍵字過濾)

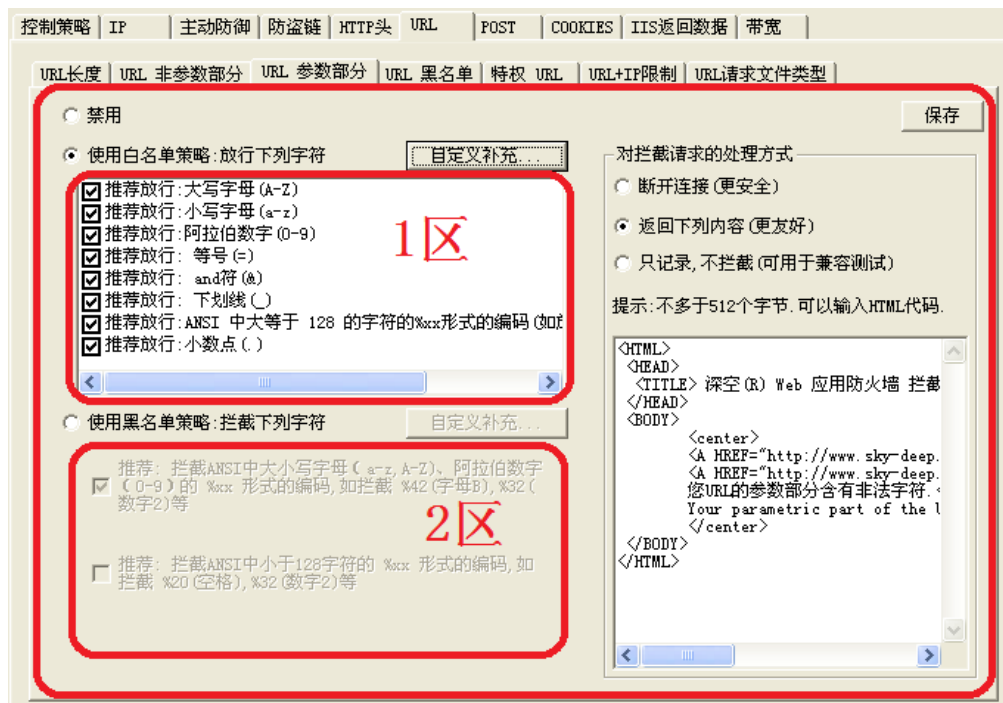
URL 參數部分是指 URL 中第一個問號後的全部內容,例如 URL:

/news/news.asp?id=100&update=2011

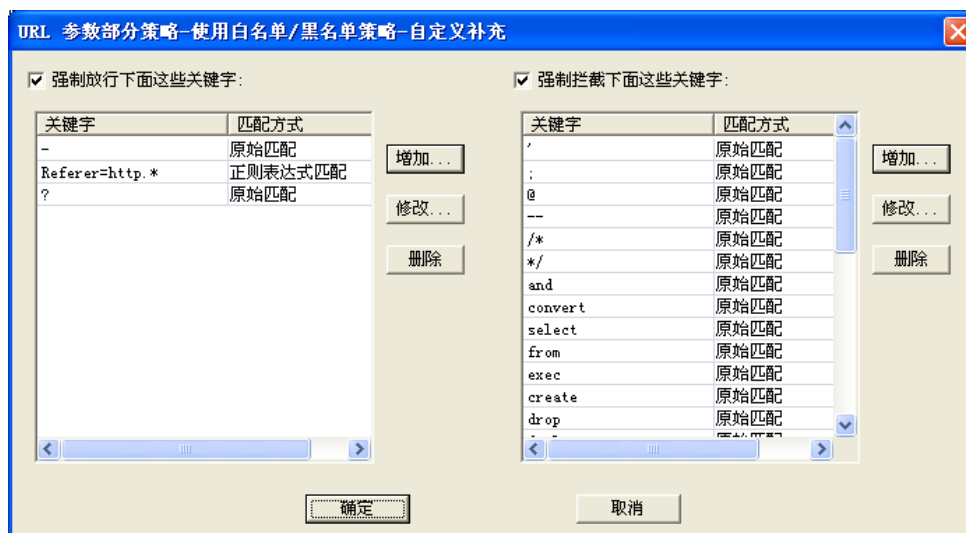
URL 參數部分為上面的紅色部分.

由於 URL 參數部分是駭客進行 SQL 注入和跨站等攻擊的重點,因此本產品提

供了 **白名單關鍵字策略** 和 **黑名單關鍵字策略** 這兩種防禦方式,並自帶了部分關鍵字,如下圖所示:



每種防禦方式使用者都可以進行 **自訂補充**,自訂補充包括**強制攔截的關鍵字**和**強制放行的關鍵字**,其中**強制攔截的關鍵字**列表中已經定義了一些常見的SQL 注入攻擊關鍵字.如下圖所示:



關鍵字匹配方式分為:**原始匹配關鍵字**(每個關鍵字最長 16 位元組)和**規則運算式匹配關鍵字**(每個關鍵字最長 64 位元組)這兩種,且匹配時都不區分大小寫.

WAF 內部對 URL 參數部分的檢測順序依次為:

如果使用白名單策略,則:

1. WAF 檢測 URL 參數部分是否存在 強制攔截的關鍵字 (如果有啟用), 如果有,就立即攔截請求.
2. WAF 檢測 URL 參數部分是否存在 白名單之外 (上圖中“1 區”定義的字元之外)的字元,如果有,就檢測是否是 強制放行的關鍵字 (如果有啟用),如果是,就跳過對該關鍵字的攔截,否則就立即攔截請求.

如果使用黑名單策略,則:

1. WAF 檢測 URL 參數部分是否存在 強制攔截的關鍵字 (如果有啟用), 如果有,就立即攔截請求.
2. WAF 檢測 URL 參數部分是否存在 黑名單之中 (上圖中“2 區”定義的字元)的字元,如果有,就檢測是否是 強制放行的關鍵字 (如果有啟用),如果是,就跳過對該關鍵字的攔截,否則就立即攔截請求.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

二十四、 URL 策略(URL 參數部分關鍵字過濾-白名單策略)

如果使用者網站中 URL 的參數部分出現的字元比較單一,或者格式比較固定,則推薦使用白名單策略.

舉例一:網站中的含參數部分的 URL 都是形如:

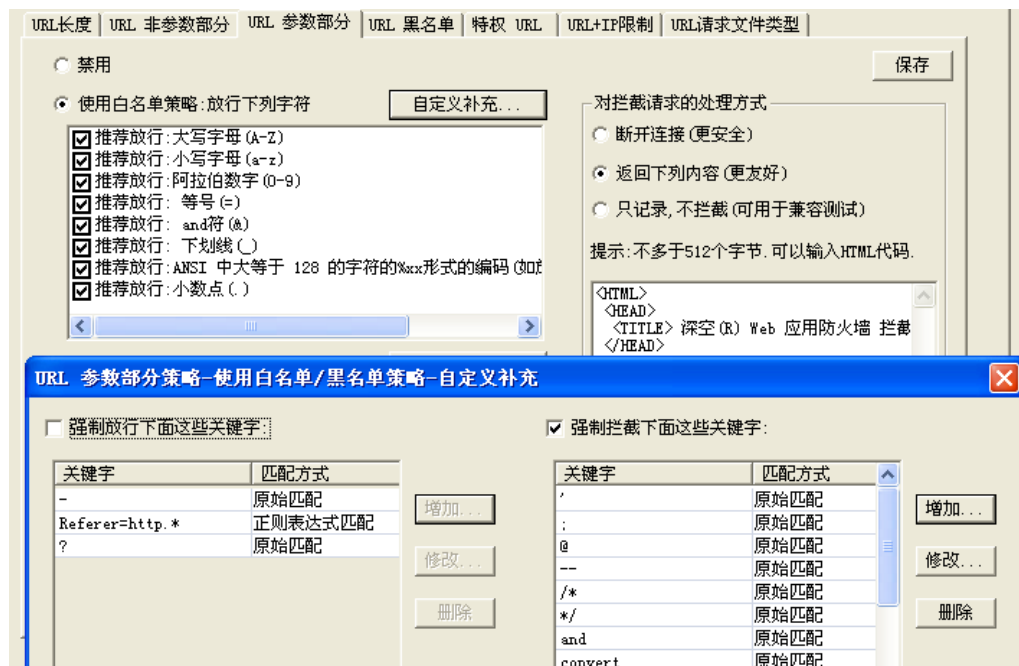
/news/news.asp?id=100&時間=2011-2

/admin/admin_news_add.asp?i_D=1_0_0&Id2=1_0_0&i 未來 3=世界

/book/book.asp?view=fa-sdf-as

分析:參數部分格式比較繁雜,但出現的字元比較單一,可以用:大小寫字母(a-z,A-Z),阿拉伯數字(0-9),and 符號(&),減號(-),底線(_),等號(=),中文 這些範圍來描述,而且,單憑這些字元,駭客無法構造出有效的攻擊語句,因為 SQL 注入/跨站腳本語句需要生效,一個很關鍵的就是需要在 URL 參數部分中輸入空格和特殊字元.(提示:對空格,駭客在 SQL 注入攻擊時可以使用閉合的注釋符代替,如 /****/ 來代替空格)

因此,這裡可以使用 白名單策略+產品自帶的自訂強制攔截關鍵字.如下圖所示:



提示:本產品推薦使用者積極開啟使用產品自帶的自訂強制攔截關鍵字.

警示:使用白名單關鍵字的用戶在自訂**強制放行的關鍵字**時,需認真考慮放行該關鍵字是否會帶來安全風險.

一些常見的危險字元有: 星號(*),小於號(<),大於號(>),at 符號(@),單引號

(), 分隔符號(|), 加號(+), 空格(), 左括弧((), 右括弧()).

舉例二:網站中的含參數部分的 URL 都是形如:

/news/news.asp?id=100&update=2011

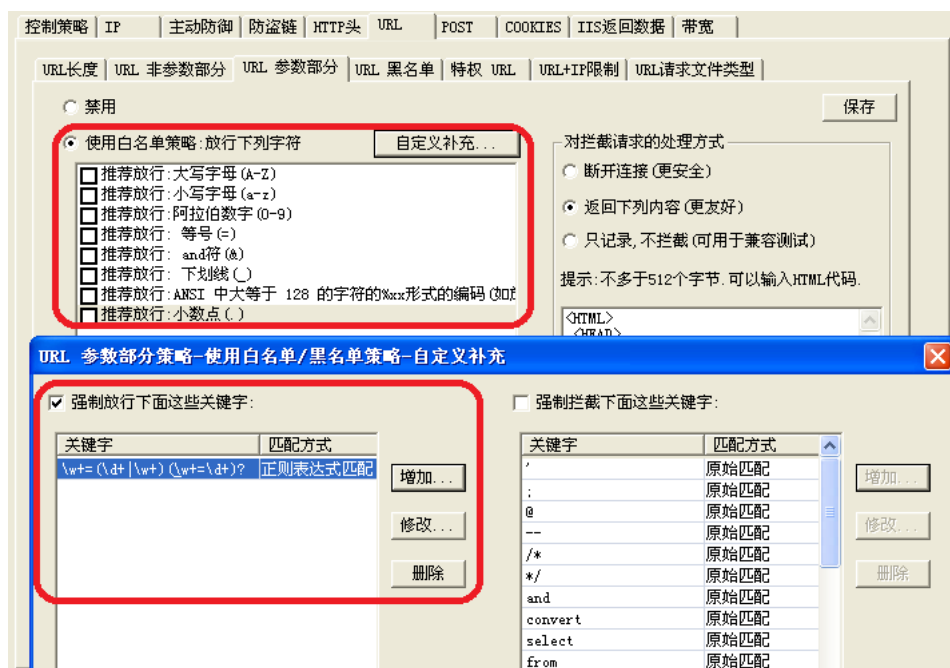
/admin/admin_news_add.asp?id=100

/book/book.asp?view=fasdfas

分析:參數部分格式比較統一,可以用規則運算式加以描述,因而可以使用 白名單策略+強制放行指定的規則運算式關鍵字.

如下所示,自帶的白名單關鍵字可以一個不選,然後點擊“自訂補充”,只啟用“放行下面這些關鍵字”,然後加入一個規則運算式關鍵字:

$\backslash w+=\backslash d+|\backslash w+)(\&\backslash w+=\backslash d+)?$



這樣設置後被保護網站的 URL 參數部分的格式將被“定死”,URL 參數部分中只有符合**強制放行關鍵字**中規則運算式的才被放行,其它一律攔截,因此大大降低了被 SQL 注入/跨站等攻擊的危險.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

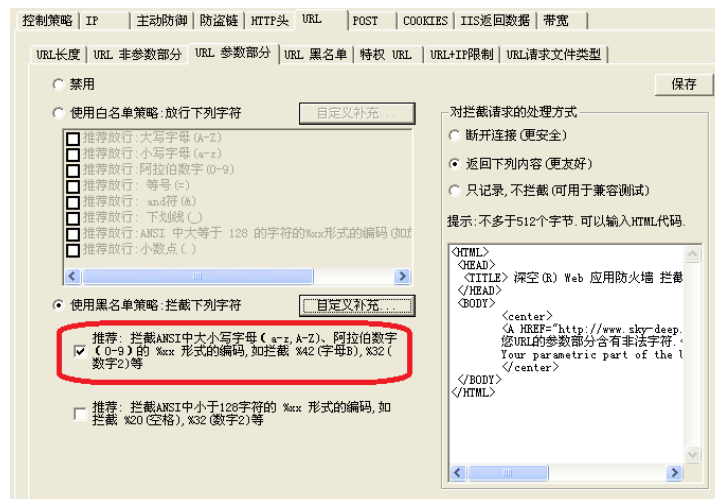
二十五、 URL 策略(URL 參數部分關鍵字過濾-黑名單策略)

如果使用者網站中 URL 的參數部分格式不固定,形式多種多樣,或者出現的字元比較繁雜,則推薦使用黑名單策略以實現 WAF 和網站正常應用的最大相容.

提示:在使用黑名單策略時,推薦使用者積極開啟使用產品自帶的自訂強制攔截關鍵字,該列表中已經定義了一些常見的 SQL 注入攻擊關鍵字.

提示:推薦使用者把產品內置的“攔截大小寫字母、阿拉伯數字 0-9 的%xx 形式的編碼”的黑名單策略開啟.該策略可以攔截駭客通過編碼變形來試圖繞過關鍵字檢測的攻擊.

如下圖所示:



保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

二十六、 URL 策略(URL 黑名單)

如果開啟本策略,WAF 將遮罩所有對處於黑名單中的 URL 及其子 URL(子目

錄)的請求。

本策略可用於保護含有重要檔的目錄(如資料庫檔所在的目錄)不被公眾訪問甚至下載。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

二十七、 URL 策略(特權 URL)

如果開啟本策略,WAF 將跳過對特權 URL 及其子 URL(子目錄)請求的 URL 類策略檢查。

本策略可用於對網站中個別特殊的與 URL 類策略衝突的 URL 進行例外處理。

警示:特權 URL 不受 URL 類策略限制,用戶應自己確保特權 URL 的安全性,WAF 對特權 URL 不進行 URL 類策略檢查(如不進行參數部分關鍵字檢查,不進行非參數部分關鍵字檢查等),因此用戶在添加特權 URL 時應當非常謹慎。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

二十八、 URL 策略(URL+IP 限制)

如果開啟本策略,WAF 將對指定的 URL 限制 IP 訪問,只有允許訪問的 IP 方能訪問該 URL 及其子 URL(子目錄)。

本策略可用於保護敏感目錄(如網站管理後臺所在的目錄,資料庫檔所在的目錄等)不被未授權 IP 訪問。

提示:使用者可以對一個 URL 最多配置 8 個可以訪問的 IP 或 IP 段(使用星號(*)萬用字元)。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

二十九、 URL 策略(URL 請求檔案類型限制)

如果開啟本策略,WAF 將對所有請求進行請求檔案類型檢查,只允許用戶設置的檔案類型被請求,其它一律攔截。

本策略可用於保護敏感檔(如資料庫檔.mdb、密碼檔.psw 等)不被公眾訪問甚至下載,也可用於攔截一些特殊拓展名的 webshell(網頁後門),如.asa、.cer、.cdx 等。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

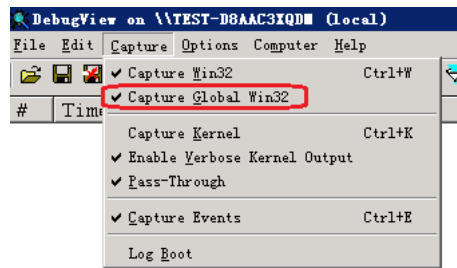
三十、 POST 策略(POST 請求內容關鍵字過濾)

如果開啟本策略,WAF 將對所有 POST 請求的內容進行關鍵字檢查,如果發現非法關鍵字,就立即攔截請求。

為方便使用者調試 POST 內容過濾關鍵字,WAF 對接收到的 POST 請求內容一律進行下列兩種方式的輸出操作:

1. WAF 檢測伺服器中是否存在調試器,如果存在,則把 POST 請求內容輸出到調試器中。

➤ 用戶在伺服器中可以用 **Dbgview** 工具([下載地址 1](#),[下載地址 2](#))查看到 WAF 即時輸出接收到的 POST 請求內容資料.注意,如果用戶在遠端桌面中運行 **Dbgview**,則必須勾選“Capture->Caputre Global Win32”方能接收到 WAF 的即時輸出資料,如下圖所示:



➤ 提示:調試完畢後,用戶應關閉 **Dbgview** 工具,以減輕 WAF 的工作量.

2. WAF 檢測伺服器 **C 盤**根目錄下是否存在 **__skd_post_debug.txt** 檔,

如果存在該檔,而且該檔 **users** 組用戶具有寫入許可權,則把 POST 請求內容附加寫入該檔中.

➤ 用戶可以打開該檔查看 WAF 接收到的 POST 請求內容資料.

➤ 提示:調試完畢後,用戶應 重命名/刪除 **C 盤**根目錄下的

__skd_post_debug.txt 檔,以減輕 WAF 的工作量.

提示:用戶可使用本策略攔截基於 POST 實施的 SQL 注入、XSS 等攻擊.

用戶可以設置**原始匹配關鍵字**(每個關鍵字最長 16 位元組)和**規則運算式匹配關鍵字**(每個關鍵字最長 64 位元組)這兩種,且都不區分大小寫,WAF 檢測關鍵字時,將分別檢測原始匹配的關鍵字和規則運算式匹配的關鍵字.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

三十一、 POST 策略(POST 請求 URL 限制)

如果開啟本策略,WAF 將限制允許 POST 請求的 URL,未明確允許的 URL 將被禁止 POST 請求.

提示: 開啟本策略可以用於阻止駭客登錄一些 Webshell (網頁後門),因為駭客登錄 Webshell 時,一般都需要提交相關口令,提交相關口令通常都需要對

Webshell 頁面進行 POST 請求方能完成。

例如,假設 index.asp 網頁被駭客在某一時間植入了後門,並且網站管理員一直未發現該後門的存在,駭客經常對該頁面進行 POST 請求來登錄後門.現在用戶開啟了本策略,只設置了對 /login.asp 頁面允許 POST 請求,其它頁面不允許 POST 請求,則任何對 index.asp 的 POST 請求都將被 WAF 攔截,因而駭客再也無法登錄該網頁後門來危害網站.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

三十二、 COOKIE 策略(COOKIE 內容關鍵字過濾)

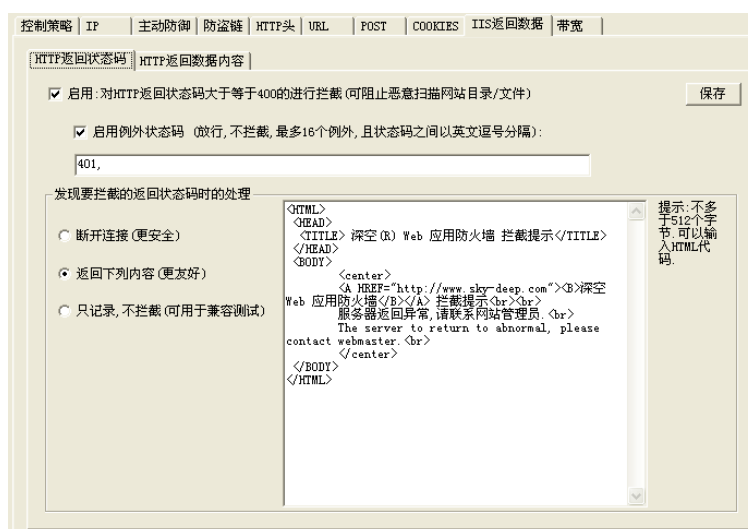
如果開啟本策略,WAF 將對所有請求的 COOKIE 進行關鍵字檢查,如果發現非法關鍵字,就立即攔截請求.

提示:用戶可使用本策略攔截基於 COOKIE 實施的 SQL 注入攻擊.

用戶可以設置**原始匹配關鍵字**(每個關鍵字最長 16 位元組)和**規則運算式匹配關鍵字**(每個關鍵字最長 64 位元組)這兩種,且都不區分大小寫,WAF 檢測關鍵字時,將分別檢測原始匹配的關鍵字和規則運算式匹配的關鍵字.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

三十三、 IIS 返回資料策略(HTTP 返回狀態碼過濾)



如果開啟本策略,WAF 將對所有 HTTP 返回狀態碼(流出 IIS 的資料)進行檢查,對非例外的而且返回狀態碼大於等於 400 的都進行攔截。

駭客攻擊時,經常會利用伺服器的一些 400 及其以上的狀態碼來分析伺服器漏洞(比如根據 web 伺服器返回的 404 狀態碼來猜解 web 目錄中敏感檔的路徑),因此,WAF 攔截這些狀態碼並發送偽造後的欺騙性狀態碼,將能夠極大地迷惑入侵者。

提示:使用者可以設置一些例外狀態碼(要求 WAF 強制放行的狀態碼)。

根據 RFC2616,HTTP 返回狀態碼分類如下(詳情請參考 RFC2616 文檔)

- 1xx: 資訊性——收到請求,繼續處理
- 2xx: 成功性——成功收到、理解並接受行動
- 3xx: 重定向——必須採取進一步行動來完成請求
- 4xx: 用戶端錯誤——請求包含錯誤語法或不能完成
- 5xx: 伺服器錯誤——伺服器沒有成功完成顯然有效的請求

具體如下:

1xx: 資訊性——收到請求,繼續處理

"100" : Continue

"101" : Switching Protocols

2xx: 成功性——成功收到、理解並接受行動

"200" : OK

"201" : Created

"202" : Accepted

"203" : Non-Authoritative Information

"204" : No Content

"205" : Reset Content

"206" : Partial Content

3xx: 重定向——必須採取進一步行動來完成請求

"300" : Multiple Choices

"301" : Moved Permanently

"302" : Found

"303" : See Other

"304" : Not Modified

"305" : Use Proxy

"307" : Temporary Redirect

4xx: 用戶端錯誤——請求包含錯誤語法或不能完成

"400" : Bad Request

"401" : Unauthorized

"402" : Payment Required

"403" : Forbidden

"404" : Not Found

"405" : Method Not Allowed

"406" : Not Acceptable

"407" : Proxy Authentication Required

"408" : Request Time-out

"409" : Conflict

"410" : Gone

"411" : Length Required

"412" : Precondition Failed

"413" : Request Entity Too Large

"414" : Request-URI Too Large

"415" : Unsupported Media Type

"416" : Requested range not satisfiable

"417" : Expectation Failed

5xx: 伺服器錯誤——伺服器沒有成功完成顯然有效的請求

"500" : Internal Server Error

"501" : Not Implemented

"502" : Bad Gateway

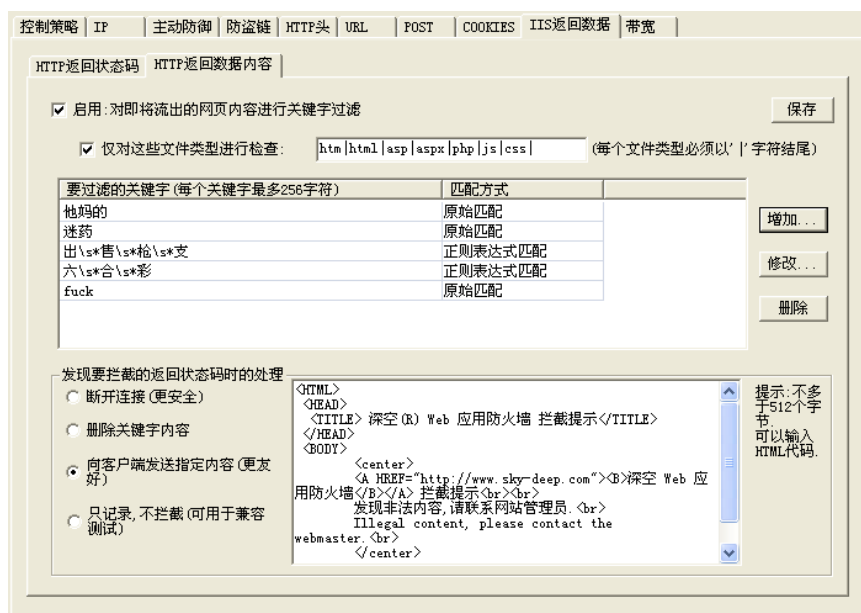
"503" : Service Unavailable

"504" : Gateway Time-out

"505" : HTTP Version not supported

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

三十四、 IIS 返回資料策略(HTTP 返回內容過濾/網頁內容過濾)



如果開啟本策略,WAF 將對所有 HTTP 返回內容(流出 IIS 的資料,即網頁內容)進行關鍵字檢查,用戶可以設置當 WAF 在網頁內容中發現非法關鍵字時採取的處理方式,目前有 4 種處理方式可供使用者選擇:

- a. **斷開連接(更安全):** 立即斷開連接。
- b. **刪除關鍵字內容:** 只刪除網頁中的非法關鍵字內容,其它內容依然正常流出.注意:因為本處理方式需要查找與剔除非非法關鍵字,所以會較慢。

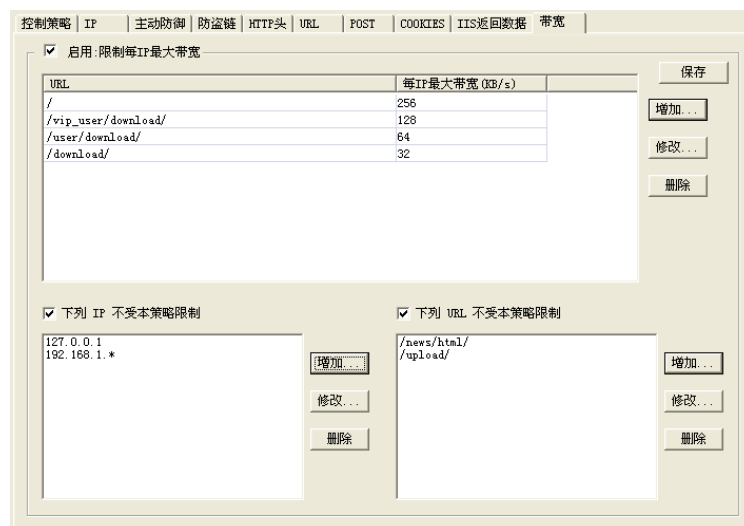
- c. 向流覽者發送指定資訊: 比如向流覽者發送“發現非法內容”等文字.
- d. 只記錄,不攔截(可用於相容測試): WAF 記錄下所有不合策略的請求但不攔截.本方式可以用來測試當前策略和網站的相容程度,這期間網站的正常運行不受影響,用戶可以逐步調試策略,直至滿意為止.

用戶可以設置**原始匹配關鍵字**(每個關鍵字最長 16 位元組)和**規則運算式匹配關鍵字**(每個關鍵字最長 64 位元組)這兩種,且都不區分大小寫,WAF 檢測關鍵字時,將分別檢測原始匹配的關鍵字和規則運算式匹配的關鍵字.

提示:推薦用戶只對指定類型的網頁(如:htm、html、asp、aspx、php、js、css)進行網頁內容檢查,這樣可以讓 WAF 減少不必要的網頁內容過濾開銷,否則 WAF 將對所有流出資料都進行過濾而不管當前資料是什麼檔案類型.

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效.

三十五、 頻寬策略



如果開啟本策略,WAF 將對指定的 URL 及其子 URL(子目錄)進行頻寬限制,除了例外 URL 和例外 IP,其它 IP 的最大訪問/下載頻寬都將被限制到用戶設置的

最大頻寬以內。

本策略的啟用可以防止因為個別 IP 佔據大量頻寬導致的影響正常用戶訪問/下載。

提示:本產品中計算頻寬的方式包括了 HTTP 的頭部等資訊,比通常意義的頻寬大 2.5 倍左右(這一數值僅僅過初步測試,未經嚴格的測試,使用者應根據實際情況進行調整).例如,假設使用者希望對/download/目錄限制每個IP最大下載頻寬為 128kb/s,則用戶應設置最大限制頻寬為 $128 \times 2.5 = 320\text{kb/s}$ 。

用戶可以設置一些不受頻寬限制的 IP/IP 段。

用戶可以設置一些不受頻寬限制的 URL 及其子 URL(子目錄)。

保存本策略配置後,點擊“控制策略”->“立即載入最新配置”後方能生效。

三十六、動態特權 IP 策略

控制策略 | IP | 主动防御 | 防盗链 | HTTP头 | URL | POST | COOKIES | HTTP返回数据 | 带宽 | 动态特权IP | 转发(反)

☒ 开启动态特权IP 保存

设置最大特权IP数: 特权时间限制(秒):

设置注册为动态特权IP的URL:

☒ 不区分大小写

设置注册成功后的提示信息:

设置注销动态特权IP的URL:

☒ 不区分大小写

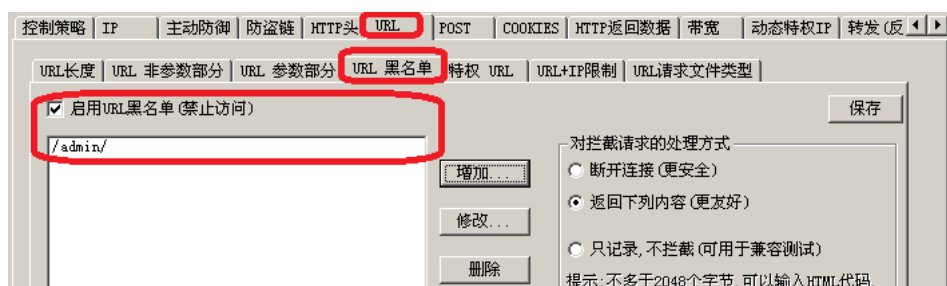
设置注销成功后的提示信息:

動態特權 IP 策略提供一種功能：使合法用戶能夠臨時不受 WAF 的各種策略限制,如直接查看到伺服器原始返回資訊、不受限制地訪問黑名單 URL 等。

例如：使用者可以將網站後臺路徑列入黑名單,同時開啟**動態特權 IP** 策略,設置一個隱蔽的進入動態特權 IP 清單的 URL,平時後臺路徑處於黑名單 URL 清單,因此駭客無法訪問,合法用戶要訪問後臺時,只需訪問一次進入動態特權 IP 清單的 URL,然後就可以不受限制地訪問到後臺路徑.下面舉例說明：

假設使用者網站後臺路徑是:www.test.com/admin/login.asp

現在 WAF 的 **URL->URL 黑名單**策略中,將 /admin/列入了黑名單,如下圖所示：



同時,開啟了 WAF 的動態特權 IP 策略,設置/zhimakaimen.kaimen 為進入動態特權 IP 清單的 URL,如下圖所示：



配置保存後,點擊“控制策略”->“立即載入最新配置”,使策略生效.

在未訪問進入動態特權 IP 的 URL 之前,訪問網站後臺:

www.test.com/admin/login.asp 將被攔截,並可看到類似如下頁面:



Web应用防火墙->拦截请求

提示: 用户可自定义该拦截页面

出现该页面的原因:

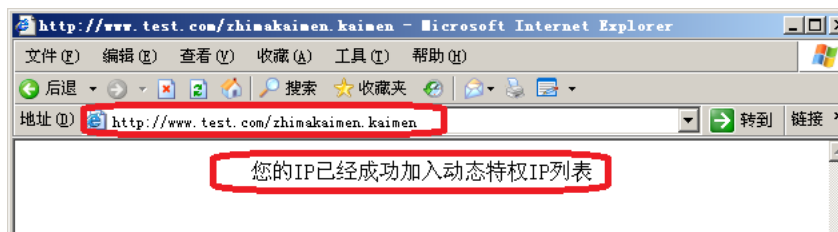
1. 该路径不允许访问;

(“日志”->“拦截日志”中记录了具体信息)

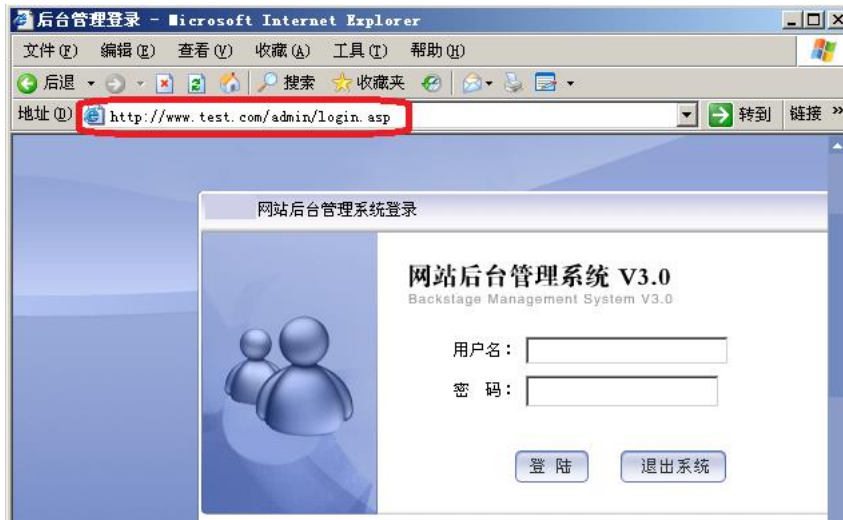
策略位置: “URL”->“URL黑名单”

技术支持:

使用者再訪問進入動態特權 IP 的 URL,WAF 將把使用者的 IP 加入動態特權 IP 清單,並可以看到如下頁面:



隨後再次訪問網站後臺: www.test.com/admin/login.asp 即可正常看到後臺登錄頁面:



完畢.

保存本策略配置後,點擊“控制策略” -> “立即載入最新配置”後方能生效.

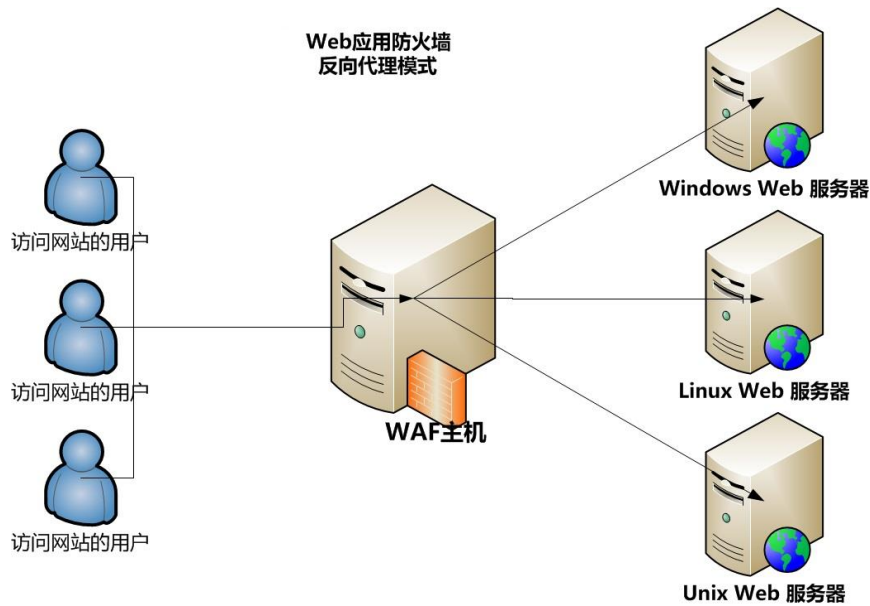
第七章 製作硬體 WAF

通過開啟 WAF 的**轉發(反向代理)**策略,可以將 WAF 所處的伺服器主機變成一台專職的硬體 web 應用防火牆(以下簡稱**硬體 WAF**)。

The screenshot shows the configuration window for the 'Forward (Reverse Proxy)' strategy. The 'Enable Forward (Reverse Proxy)' checkbox is checked. The 'Forward to IP' is set to 127.0.0.1 and the 'Port' is set to 81. Below, there are options for customizing URL parameters and forwarding timeouts, all of which are currently unchecked. A 'Restore Default' button is available for the timeout settings.

Control Strategy	IP	Active Defense	Anti-DDoS	HTTP Header	URL	POST	COOKIES	HTTP Return Data	Bandwidth	Forward (Reverse Proxy)
☒ 启用转发(反向代理) 保存 转发到IP: 127.0.0.1 端口: 81 以下配置如果不熟悉请保持默认 ☐ 自定义URL参数部分代码页 65001 ☐ 自定义转发超时设置 转发连接超时(毫秒) 60000 转发发送超时(毫秒) 30000 转发接收超时(毫秒) 30000 恢复默认										

如開啟**轉發(反向代理)**策略,WAF 將把清洗後的請求轉發給指定 IP 的指定埠,並把返回資料經清洗後回傳給請求者.使用者可以通過開啟該策略實現對非 windows 系統的 web 應用安全防護,如下圖所示：



一、 硬體準備

一台可安裝 windows 伺服器作業系統的 PC 機或伺服器,當作 WAF 的硬體.

- **處理器：** 至少 Intel Pentium III,推薦雙核以上的多核多執行緒 CPU.
- **記憶體：** 至少 256MB,推薦 2G 以上.
- **硬碟：** 至少剩餘空間在 10G 以上 ,推薦剩餘空間 15G 以上.

二、 軟體準備

- **Windows** 伺服器作業系統一套,如:

Windows Server 2003 Enterprise Edition SP2

Windows Server 2008 Enterprise Edition SP2/R2

Windows Server 2012 Enterprise Edition

- 深空 **web** 應用防火牆系統軟體一套.

三、 部署方式

以下步驟描述基於假設:

聞道:

192.168.1.1

硬體 WAF (Windows 伺服器作業系統):

192.168.1.2

web 伺服器(Linux 作業系統)IP:

192.168.1.3,HTTP 服務埠:80

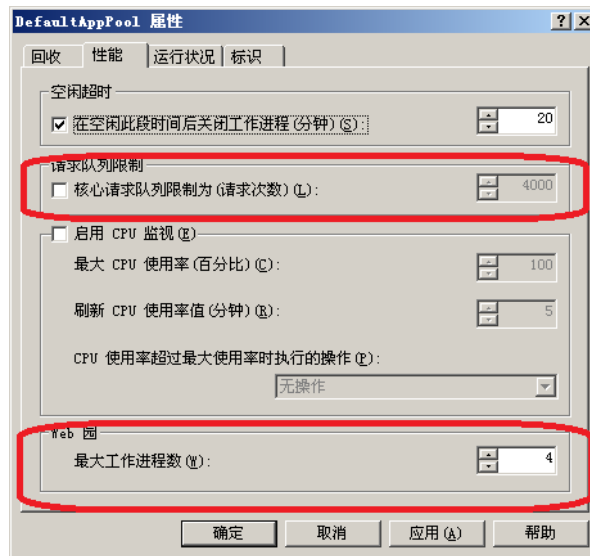
要求:

在 192.168.1.2 上部署 WAF,從而把 192.168.1.2 改造成一台硬體 WAF,然後用它保護 192.168.1.3 這個 Linux 作業系統 web 伺服器的 HTTP(80 埠)web 服務.

下麵是操作步驟:

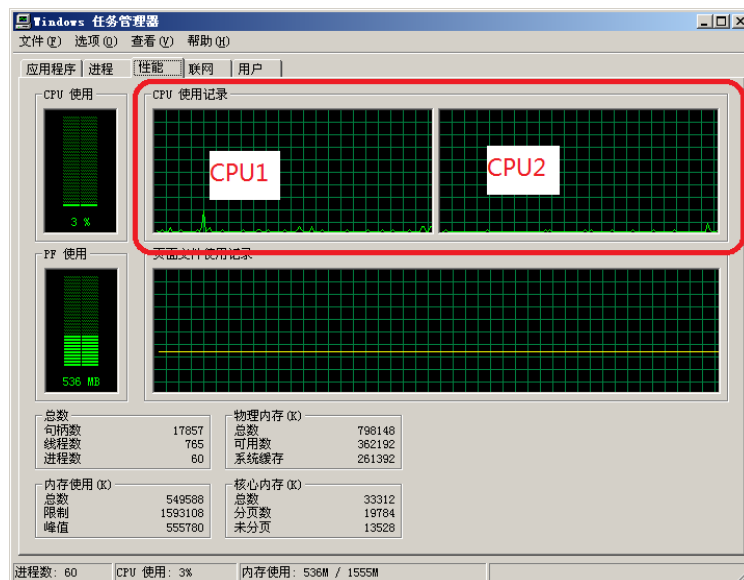
- ❖ 第一步: 在硬體主機(192.168.1.2)上安裝好 windows 伺服器作業系統,並安裝好 IIS(如果是 64 位元系統或者 IIS7.0 以後版本,請參閱[注意事項](#)),然後按下面的說明調整預設應用程式池屬性配置:

1. 取消請求佇列限制,如下圖所示;

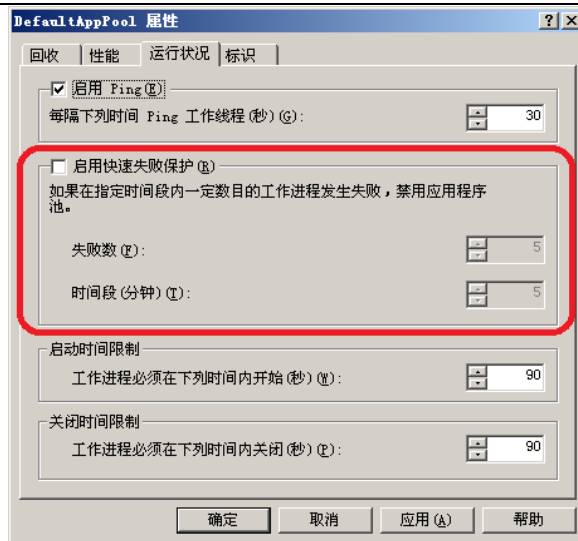


2. 設置web 園最大工作進程數: 設置為工作管理員所見CPU 總核心數的 2 倍或 4 倍,如上圖所示.

下圖工作管理員所示 CPU 總核心數為 2,則最大工作進程數設置為 4 或 8 (注意: 為增強併發性,無論 CPU 總核心個數為多少,此值都不得小於 4) .



3. 關閉快速失敗保護,如下圖所示:



4. 完畢,點擊“確定”保存。

❖ **第二步:**在硬體主機(192.168.1.2)上,把下面的內容另存為 reg 檔,也就是註冊表檔,然後按兩下導入:

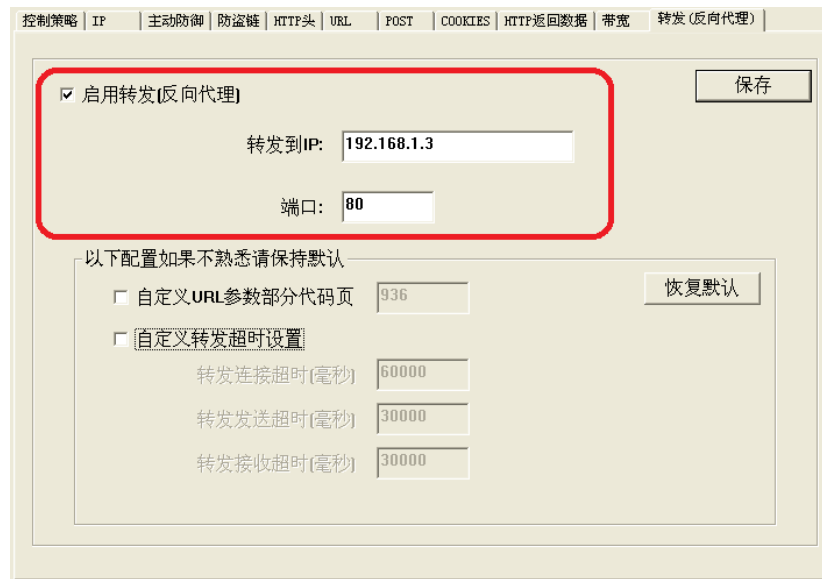
Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"TcpMaxHalfOpen"=dword:000001f4
"SynAttackProtect"=dword:00000001
"TcpMaxHalfOpenRetried"=dword:00000190
"EnablePMTUDiscovery"=dword:00000000
"TcpMaxPortsExhausted"=dword:00000005
"KeepAliveTime"=dword:00000bb8
"KeepAliveInterval"=dword:000003e8
"TcpMaxDataRetransmissions"=dword:00000002
"NoNameReleaseOnDemand"=dword:00000001
"DefaultTTL"=dword:00000040
"TcpTimedWaitDelay"=dword:00000005
"TcpNumConnections"=dword:00ffffff
"MaxUserPort"=dword:0000ffff
"MaxHashTableSize"=dword:00010000
"MaxFreeTcbs"=dword:ffffff
```

注意:導入完成後,必須重新開機作業系統。

❖ **第三步:** 在硬體主機(192.168.1.2)上安裝深空 web 應用防火牆系統軟體,並開啟轉發(反向代理)策略.轉發 IP: 192.168.3 ,轉發埠: 80,保存

配置,並立即載入最新配置.如下圖所示:



- ❖ **第四步:** 在閘道處,將原來發往 192.168.1.3 的 80 埠資料改成發往硬體 WAF 的 IP 192.168.1.2 的 80 埠.
- ❖ **第五步:搭建完畢.**此時 192.168.1.2 已經可以對 192.168.1.3 進行 web 應用防護.

四、 其它選項說明

➤ 自訂 URL 參數部分內碼表

WAF 預設配置 URL 參數部分內碼表: **65001**(也就是 UTF8).

WAF 所轉發的 URL 參數部分中,如果含有跟編碼有關聯的資訊(比如 URL 參數部分出現了中文文字),而且該資訊不是 UTF8 編碼的,則使用者必須在此調整內碼表.全球各語系編碼內碼表清單可參考:

[http://msdn.microsoft.com/en-us/library/dd317756\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/dd317756(VS.85).aspx)

下圖所示為修改 URL 參數部分內碼表為 **936**(GB2312 編碼).

➤ 自訂轉發超時設置

轉發請求時,涉及到連接、發送、接收超時時間設置,用戶可以在此調整 WAF 默認超時時間。

默認連接逾時: 60000 毫秒(60 秒).

默認發送超時: 30000 毫秒(30 秒).

默認接收超時: 30000 毫秒(30 秒).

提示：保存本策略配置後,點擊“控制策略” -> “立即載入最新配置”後方能生效.

第八章 日誌類操作

本產品中的日誌分為 **WAF 攔截日誌**、**管理日誌**、**錯誤日誌**和**產品日誌**這四種。

其中,產品日誌只有 **產品管理員使用者** 使用 **管理員用戶端** 方能查看。

其中,對 **WAF 攔截日誌**,使用者可以控制日誌記錄的物件,即要求 **WAF** 哪些攔截日誌要記錄,哪些攔截日誌不要記錄。

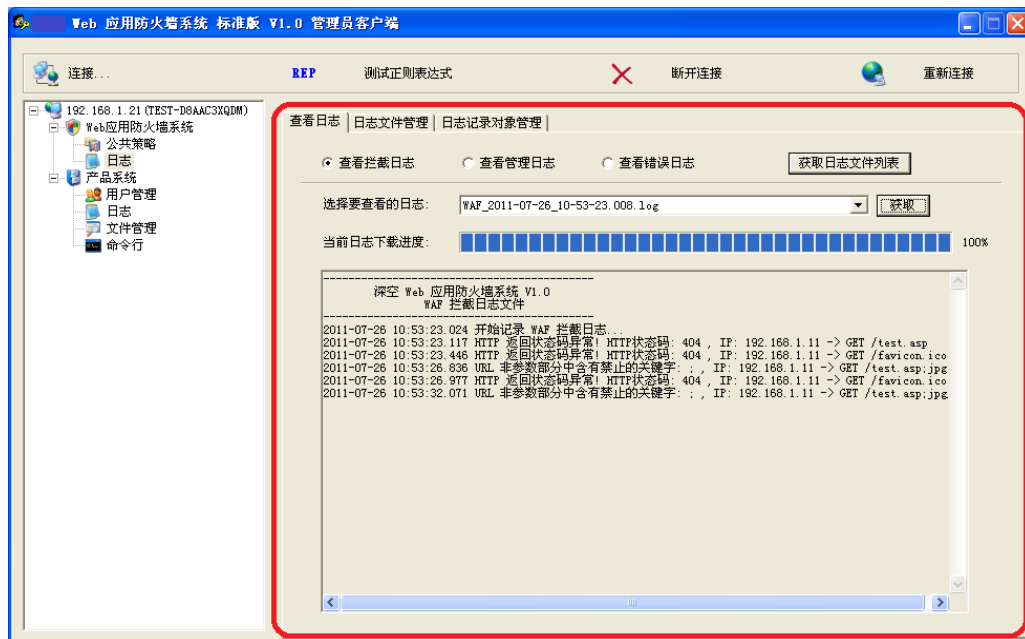
WAF 攔截日誌: 記錄了 **WAF** 攔截的每一條請求的詳細資訊,包括:攔截時間(精確到毫秒)、攔截的原因、關鍵字(如果有)、源 **IP** 位址、請求方式、請求的 **URL** 等資訊。

管理日誌: 記錄了策略執行和使用者的對策略的修改操作資訊,包括:當前策略對應用戶的登錄/退出的時間(精確到毫秒)、修改時間(精確到毫秒)、執行修改操作的用戶名、修改的內容等資訊。

錯誤日誌: 記錄了當前策略的在任一過程中發生的錯誤資訊。

產品日誌: 記錄了產品運行和管理員修改產品相關配置的資訊,包括:產品進程的啟動時間、結束時間、退出時間、退出的原因、管理員/普通用戶的登錄時間、管理員/普通用戶的退出時間、各個策略的載入情況、私有策略的創建/刪除情況等資訊。

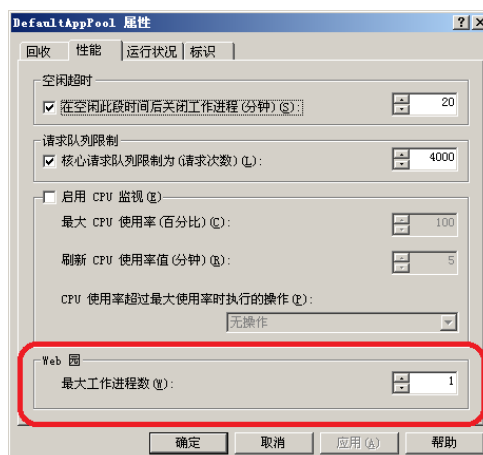
一、查看日誌檔內容



如上圖所示,使用者可以通過“查看日誌”來查看各種日誌檔的內容。

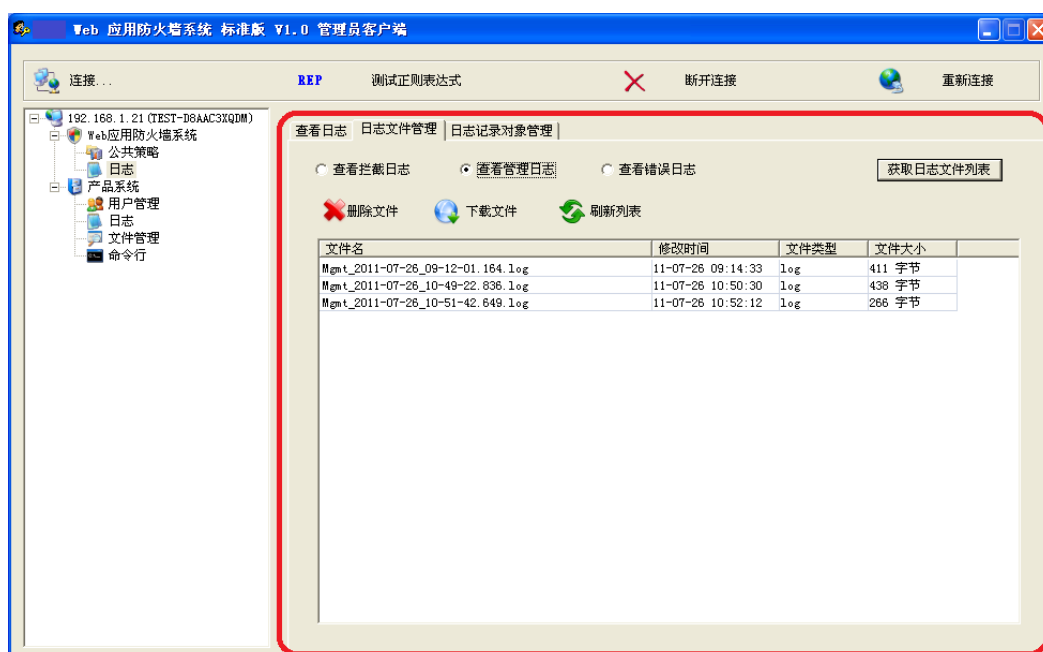
提示:使用者需點擊“獲取日誌檔清單”後,才能列出當前的日誌檔清單。

提示:因為本產品設計成一個 IIS 工作進程(如 w3wp.exe)對應一個 WAF 攔截日誌檔,所以在預設情形下,1 個網站對應的最新 WAF 攔截日誌只有 1 個。對 IIS 的 6.0 及以後版本,如果某網站所在應用程式池的 Web 園設置的“最大工作進程數”大於 1 個,則該網站對應的最新 WAF 攔截日誌檔也將可能大於 1 個。



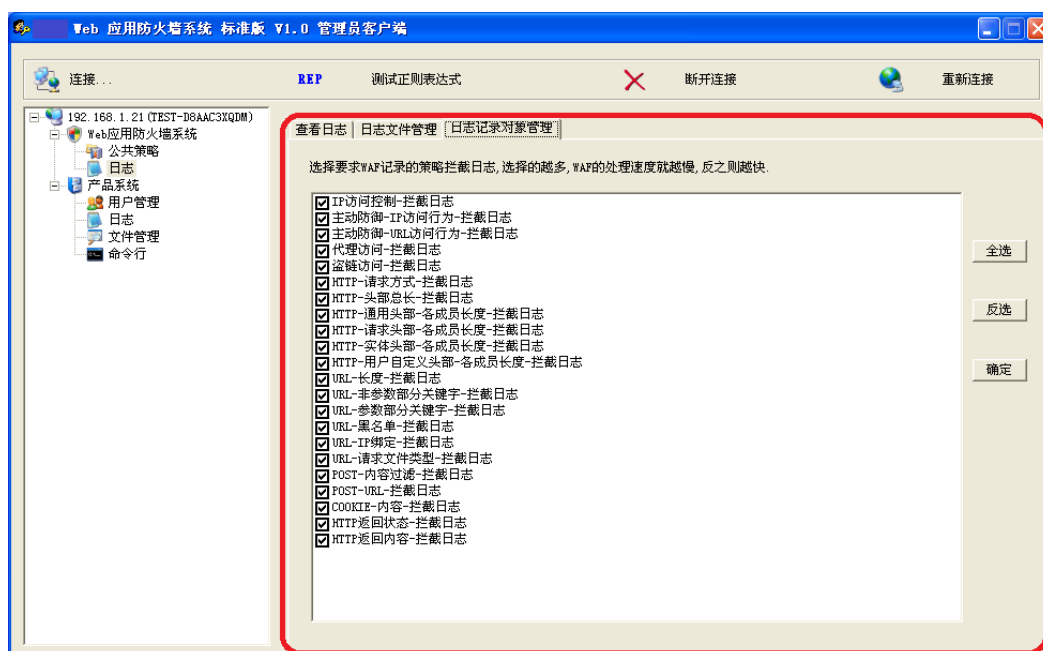
提示:在日誌顯示區,用戶端會每隔 5 秒自動刷新一次日誌。

二、 日誌檔管理



如上圖所示,使用者可以通過“日誌檔管理”來查看、刪除（可批量刪除）、下載（可批量下載）各種日誌檔。

三、 日誌記錄物件管理



如上圖所示,使用者可以通過“日誌記錄物件管理”來選擇需要日誌記錄的

物件,使用者可以控制日誌記錄的物件,即要求 WAF 哪些攔截日誌要記錄,哪些攔截日誌不需要記錄.

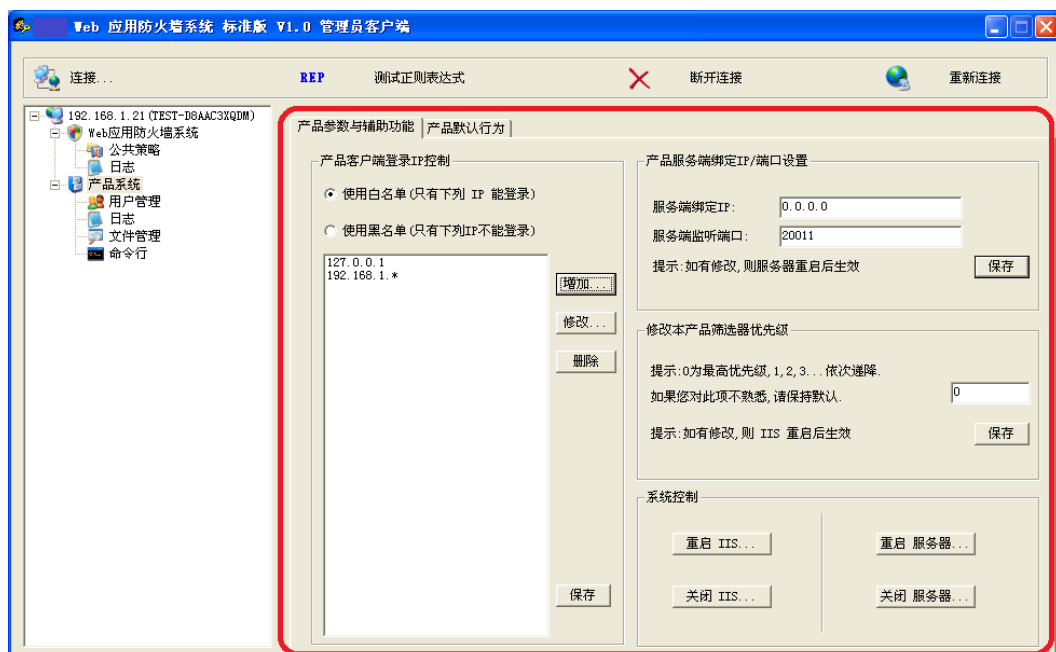
提示:使用者可以根據自身情況選擇需要日誌記錄的物件,原則上應儘量少選,因為需要日誌記錄的物件越多,WAF 的速度就越慢.

第九章 產品系統操作

如下圖所示,左邊樹形清單中的”產品系統”,該系統只有 產品管理員使用者 使用 管理員用戶端 才能查看。



一、產品用戶端登錄 IP 限制



如上圖所示,使用者可以對產品用戶端的登錄 IP 進行限制,以增強產品的安全性.本產品提供了黑名單 IP 和白名單 IP 這兩種策略來限制用戶端的登錄範圍。

使用黑名單 IP 時,只有黑名單中的 IP 不可登錄;使用白名單 IP 時,只有白名單中的 IP 才允許登錄,其它一律禁止登錄。

用戶可以設置一個或多個 IP/IP 段為黑名單或白名單。

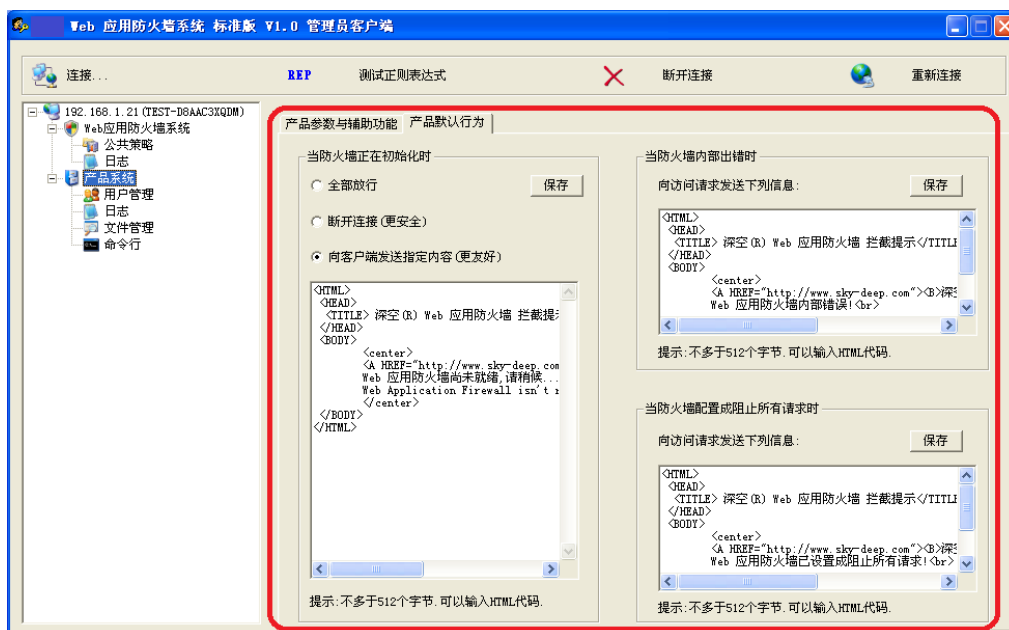
二、 產品服務端綁定 IP/埠

產品預設在所有網卡上監聽 20011 埠,使用者可以根據自身的情形進行修改綁定 IP 或監聽的埠。

三、 系統控制

本產品的管理員用戶端提供了對作業系統的一些快捷控制按鈕,包括“重啟 IIS”、“關閉 IIS”、“重啟伺服器”、“關閉伺服器”。

四、 產品預設行為



如上圖所示,用戶可以對“當防火牆正在初始化時”、“當防火牆內部出錯

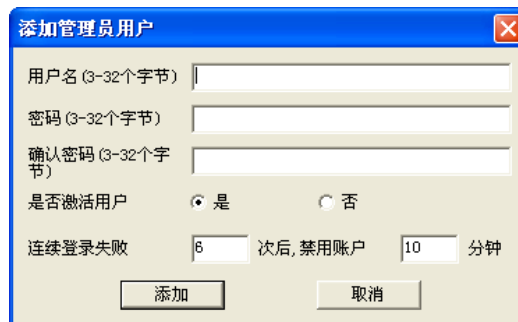
時”、“當防火牆配置成阻止所有請求時”這三種情況向流覽者發送的資訊作出自定義。

特別地,對“當防火牆正在初始化時”這種情形,用戶可以設置 WAF 的處理方式為下列之一:

- a. **全部放行:** 策略初始化完成前,放行所有請求。
- b. **斷開連接(更安全):** 立即斷開連接。
- c. **向流覽者發送指定資訊:** 如向流覽者發送“WAF 正在初始化,請稍候再刷新...”。

五、 用戶管理

在”用戶管理”中,管理員用戶可以重設自己的用戶名和密碼,也可以添加、刪除、修改一個管理員/普通用戶等,如下圖所示添加管理員用戶:



管理員用戶可以設置一個用戶最多可連續登錄失敗的次數,以及超出此次時臨時禁用該用戶的分鐘數.例如,產品預設對一個連續登錄失敗 6 次的用戶會臨時禁用其 10 分鐘,在禁用時間內,此用戶將被拒絕登錄,即使輸入正確的用戶名和密碼。

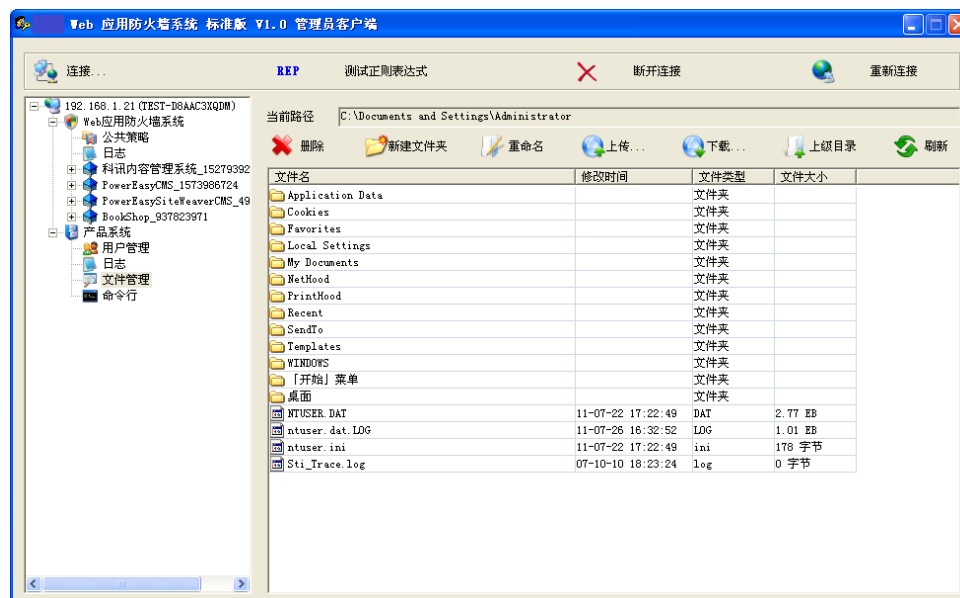
提示,在達到最多允許的連續登錄失敗次數之前,如果有一次成功登錄,則該用戶可連續登錄失敗的次數又將恢復成管理員用戶指定的次數(默認為 6 次)。

在創建普通用戶時,管理員用戶可以給普通用戶設置相關的許可權,也就是該普通用戶能夠管理的網站(私有策略).如下圖所示:



普通用戶使用普通用戶用戶端登錄時,只能看到它有權管理的網站(私有策略),並且不具備“產品系統”.本產品的普通使用者這一概念方便 IDC 使用者開設 **Web 防火牆網路安全增值服務**.

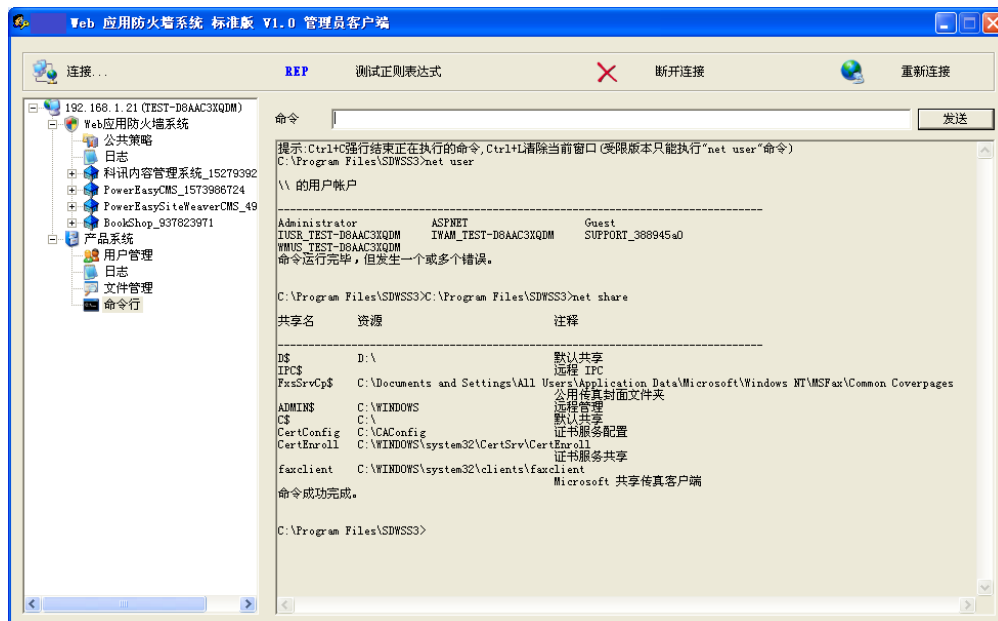
六、 文件管理



如上圖所示,在“檔管理”中,用戶可以對伺服器中各個硬碟分區上的檔進行

管理,包括：刪除、新建資料夾、重命名、上傳檔/資料夾（含批量操作）、下載檔案/資料夾（含批量操作）、刷新等。

七、 命令列



如上圖所示,在“命令列”中,用戶可以遠端模擬執行 cmd 命令,如 net user、net share、tasklist、ping 等。

第十章 不同環境下的注意事項

若本產品即將安裝在 64 位元作業系統上,或者即將安裝在 IIS7.0 及其以後版本的伺服器中時,在安裝產品前,須進行如下所述的額外配置.

若本產品安裝在網域控制站 (Domain Controller) 上,[請跳到這裡](#) .

一、 Windows XP x64 / Windows Server 2003 x64 作業系統

首先打開 cmd.exe,切換到 c:\inetpub\AdminScripts 目錄,然後在命令列中依次輸入如下兩行命令:

命令一 (僅限 Windows Server 2003 x64 系統, Windows Vista 及其以後的系統無需執行此命令):

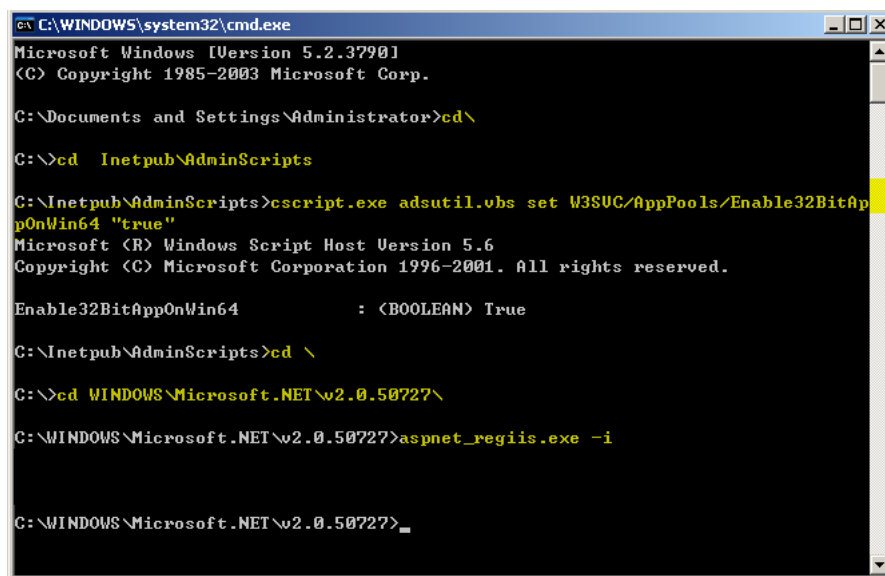
```
cscript.exe adsutil.vbs set W3SVC/AppPools/Enable32BitAppOnWin64 "true"
```

命令二:

```
%SYSTEMROOT%\Microsoft.NET\Framework\<version>\aspnet_regiis.exe -i
```

(注意: "%SYSTEMROOT%" 是系統目錄,一般是 c:\windows " <version>" 是 asp.net 版本號,視自身網站所運行的 .net 版本而定)

如下圖所示:



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd\

C:\>cd Inetpub\AdminScripts

C:\Inetpub\AdminScripts>cscript.exe adsutil.vbs set W3SVC/AppPools/Enable32BitApp
pOnWin64 "true"
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

Enable32BitAppOnWin64          : <BOOLEAN> True

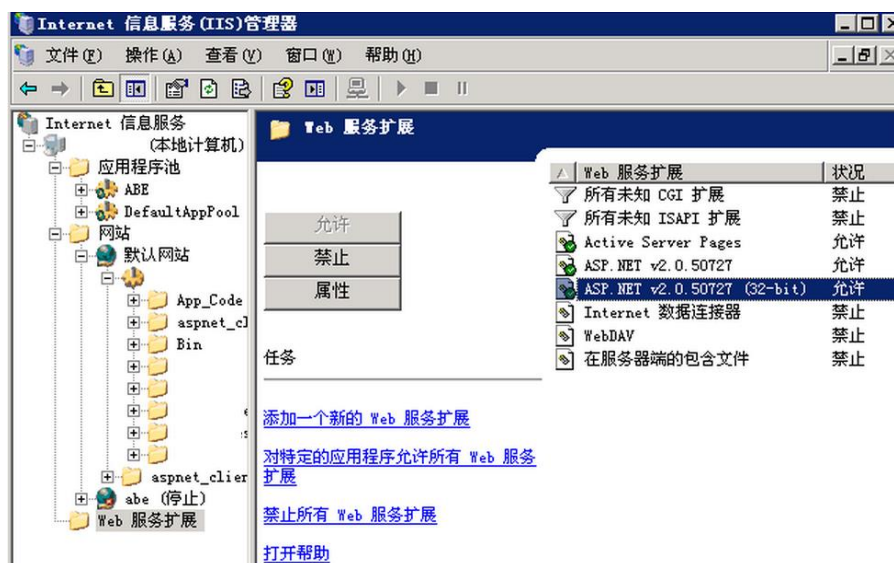
C:\Inetpub\AdminScripts>cd \

C:\>cd WINDOWS\Microsoft.NET\w2.0.50727\

C:\WINDOWS\Microsoft.NET\w2.0.50727>aspnet_regiis.exe -i

C:\WINDOWS\Microsoft.NET\w2.0.50727>
```

2.設置 ASP.NET 32 位元的 web 服務拓展為允許,如下圖所示:

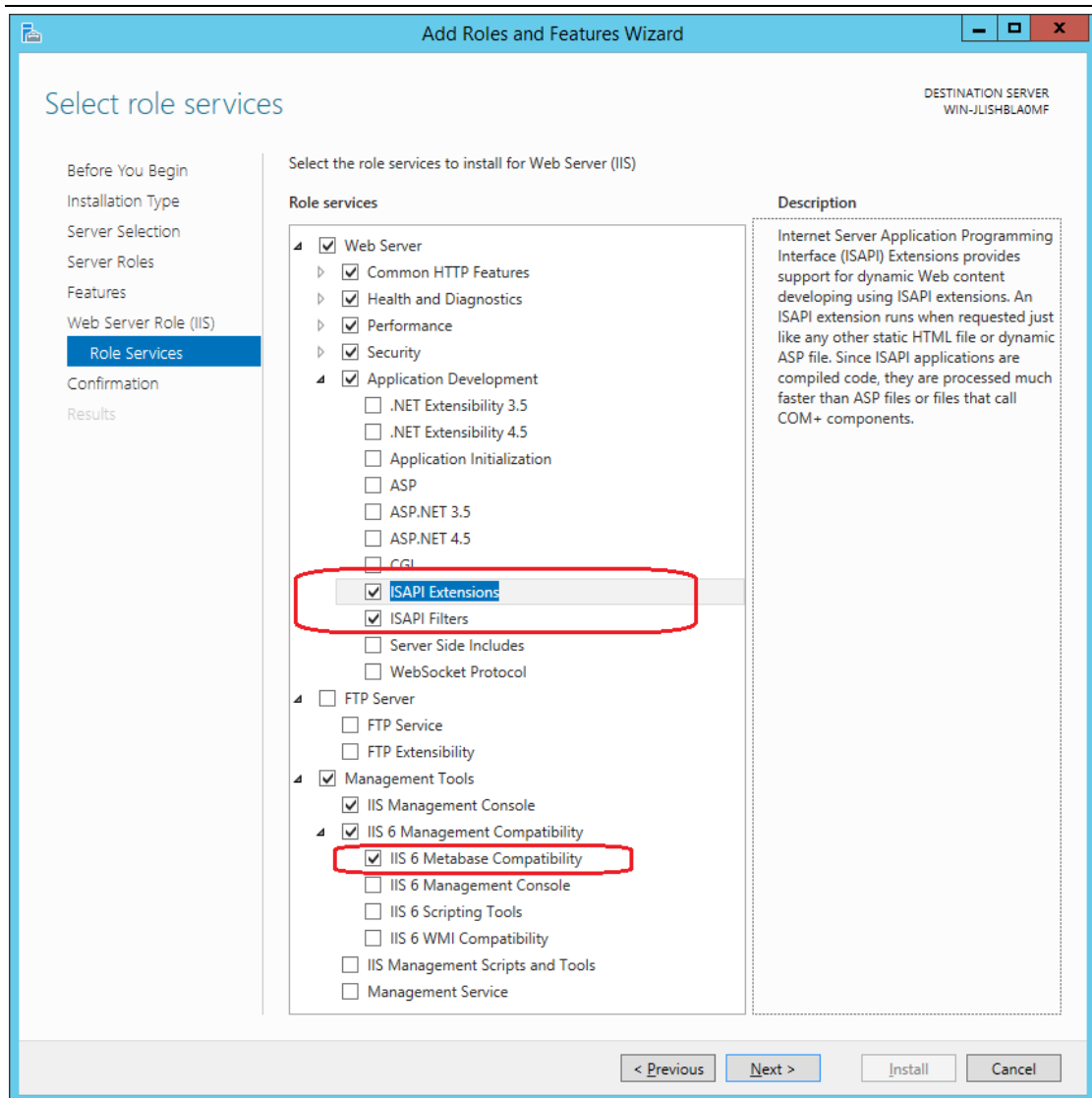


完成配置.

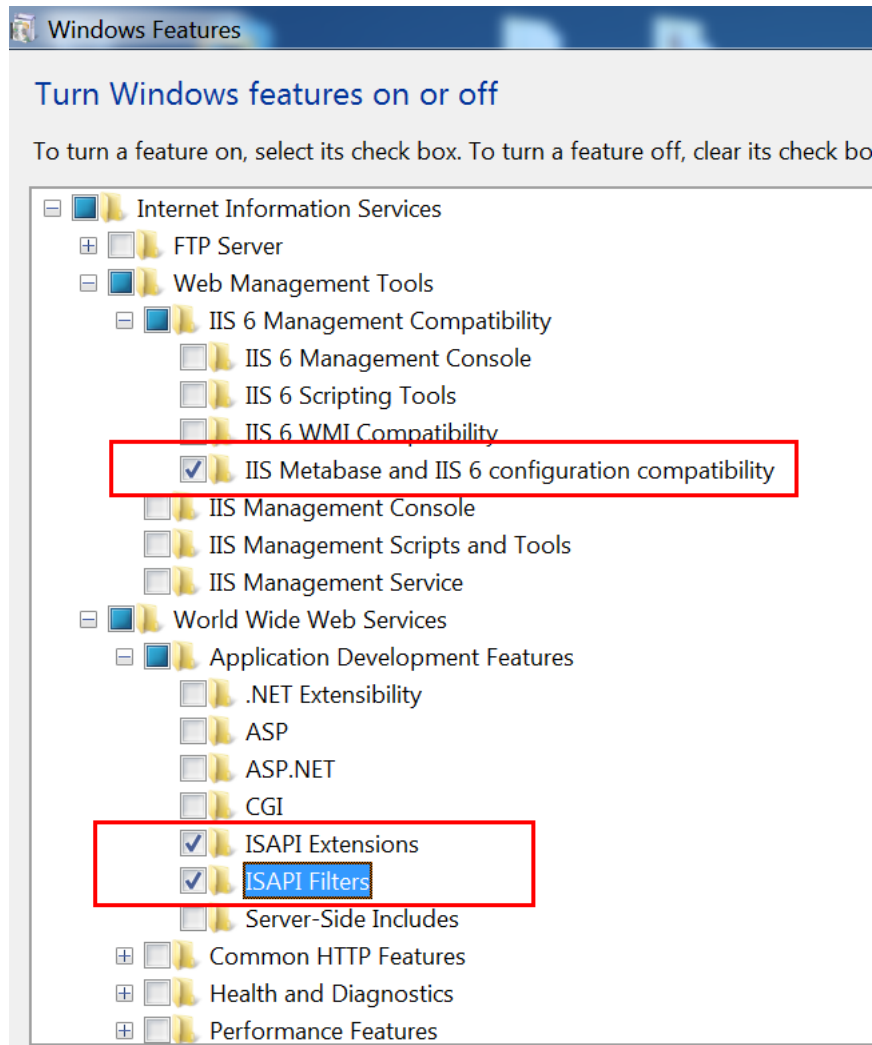
二、 IIS7.0 及其以後版本的環境中

在 IIS7.0 及其以後版本的環境中安裝本產品時, **IIS6 Metabase Compatibility** (**IIS6 中繼資料庫相容性**)、**ISAPI Extensions** (**ISAPI 拓展**) 和 **ISAPI Filter** (**ISAPI 篩選器**) 這三個角色必須確保已安裝,否則在安裝時會提示未安裝 IIS 或者後期 WAF 運行不正常.

下圖為 Windows Serve 2012 R2 添加角色和功能嚮導的截圖,紅色方框所示的 **IIS6 Metabase Compatibility** (**IIS6 中繼資料庫相容性**)、**ISAPI Extensions** (**ISAPI 拓展**) 和 **ISAPI Filter** (**ISAPI 篩選器**) 必須勾選並安裝.



下圖為 Windows 7 控制台->程式->“ 打開/關閉 Windows 角色” 的截圖, 紅色方框所示的 **IIS6 Metabase Compatibility** (IIS6 中繼資料庫相容性)、**ISAPI Extensions** (ISAPI 拓展) 和 **ISAPI Filter** (ISAPI 篩選器) 必須勾選並安裝.



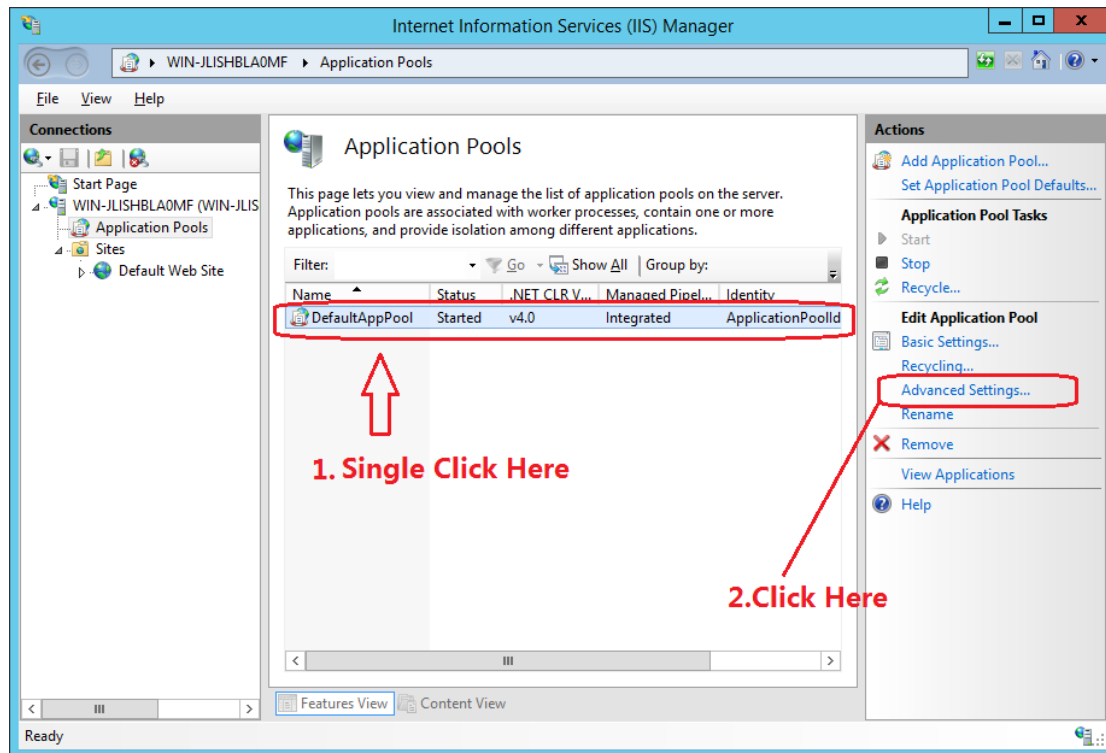
三、 Vista/2008 及以後的 x64 作業系統

在 Vista/2008 及以後的 64 位元作業系統中運行時,應用程式池必須設置成 32 位元應用程式相容模式: 應用程式的“高級設置”屬性中,把 **Enable 32-Bit Applications** (啟用 32 位元應用程式) 設置成 **True**.

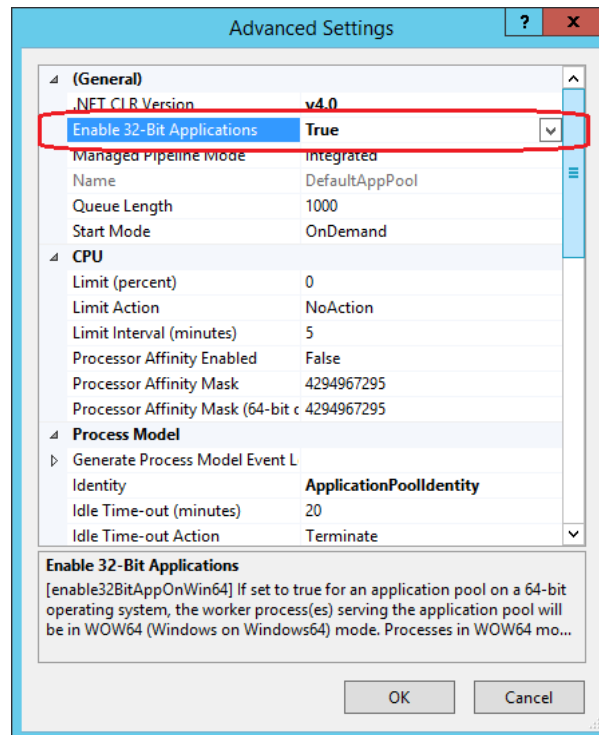
注意: 下面的操作建立在假設被保護網站的應用程式池是預設的應用程式池 (DefaultAppPool) 的基礎上. 如果被保護網站的應用程式池不是預設的應用程式池,請根據後面的示例,對相應的應用程式池進行配置.

1.打開 IIS 管理工具

2.按下圖所示操作



3.彈出類似下圖方框,按圖中所示把 **Enable 32-Bit Applications**（啟用 32 位元應用程式）設置為 **True**,隨後按一下"OK"關閉對話方塊,完成配置.



四、網域控制站（Domain Controller）上的額外操作

如果本產品安裝在域環境的網域控制站（Domain Controller）上,則要檢測 IIS 中的應用程式池標識(預設為 NETWORK_SERVICE 帳戶)是否是 IIS_WPG(Windows Server 2003)/IIS_IUSRS(Windows Vista 及以後) 組的成員.檢測方法如下:

打開 cmd.exe,輸入下面的命令:

對 Windows Server 2003 系統,執行下面的命令:

```
Net localgroup IIS_WPG
```

對 Windows Vista 及以後的系統,執行下面的命令:

```
Net localgroup IIS_IUSRS
```

查看執行結果中是否有應用程式池標識帳戶,如果應用程式池標識為上述組的成員,則下面操作可跳過.

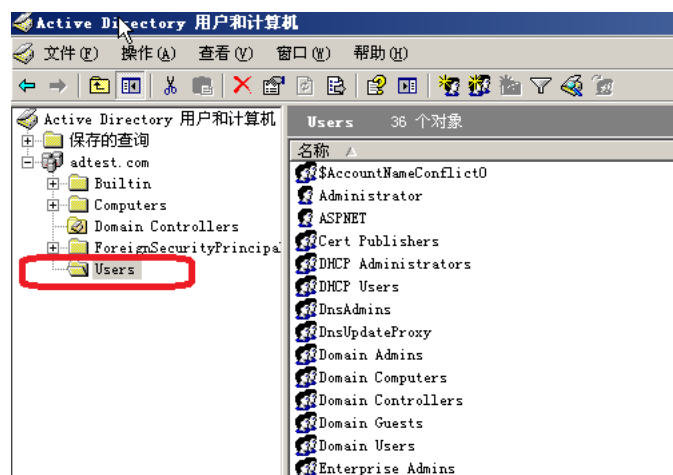
否則,新創建一個帳戶,並把它加入到上述組中(Windows Server 2003 下加入 IIS_WPG 組,Windows Vista 及以後則加入 IIS_IUSRS 組).假設新創建帳戶的帳戶名為 AppPoolUser,則操作方法示例如下:

1. 首先打開 cmd.exe,輸入並執行下面的命令:

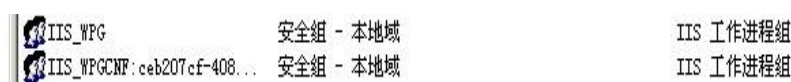
```
Net user AppPoolUser Password123 /add
```

2. 然後按如下所述操作:

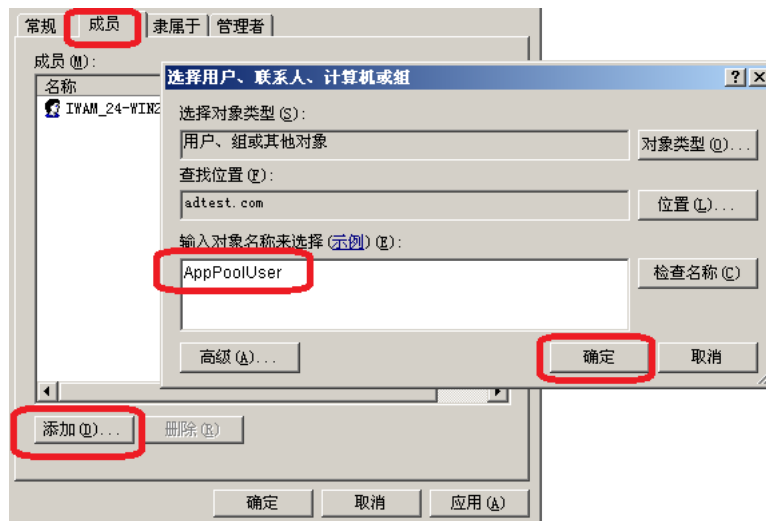
首先打開控制台->管理工具->Active Directory 使用者和電腦->Users



查看是否有類似 IIS_WPGCNF:xxxxxxxx-....的 IIS 工作進程組,如下圖所示:



如果有,則按兩下這個 IIS_WPGCNF:xxxxxxxx-....使用者組,選“成員”選項卡,然後把 AppPoolUser 用戶加進去,如下圖所示:



然後點擊“確定”保存並關閉對話方塊。

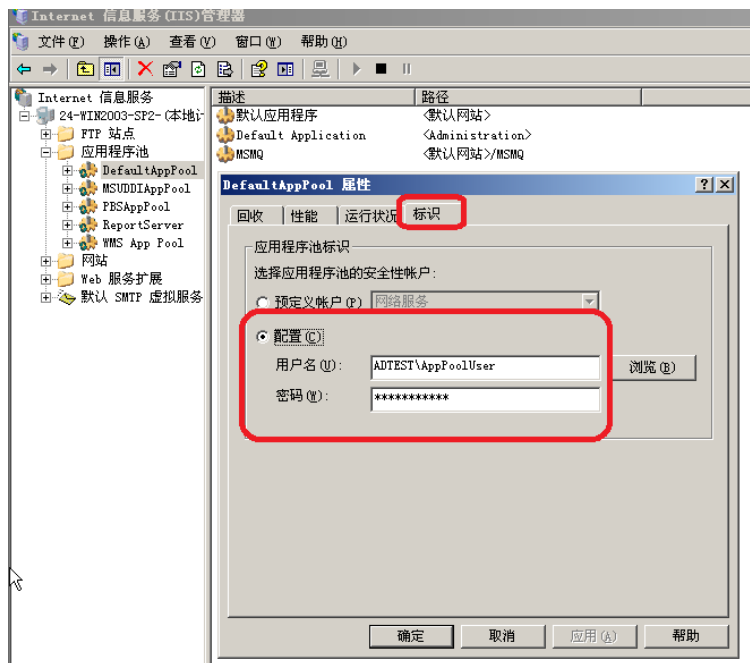
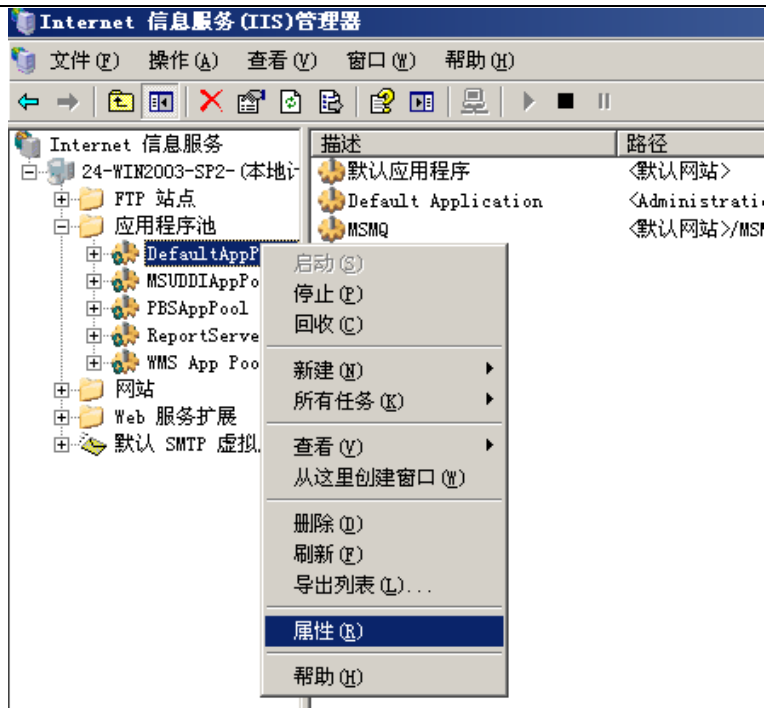
對 Windows Server 2003 系統,再執行下面的命令:

```
Net localgroup IIS_WPG AppPoolUser /add
```

對 Windows Vista 及以後的系統,再執行下面的命令:

```
Net localgroup IIS_IUSRS AppPoolUser /add
```

3. 再把應用程式池的標識改成 AppPoolUser ,如下圖所示(Windows Server 2003 中的操作截圖):



4. 最後重啟 IIS(命令列下輸入 iisreset).

5. 完畢.

第十一章 使用審計策略

本產品對自身安裝目錄下的所有檔都提供了物件訪問審計策略支援.該項功能需要作業系統啟用物件訪問**審計策略**的配合,使用者可根據自身安全要求決定是否啟用該策略.

該功能簡介：非管理員組（administrators）使用者訪問產品安裝目錄下的檔,都將失敗,且該行為會被記錄到作業系統安全性記錄檔中.

一、 啟用對象訪問審計策略

預設下,作業系統不打開該項審計,要啟用該項審計,按如下方式操作：

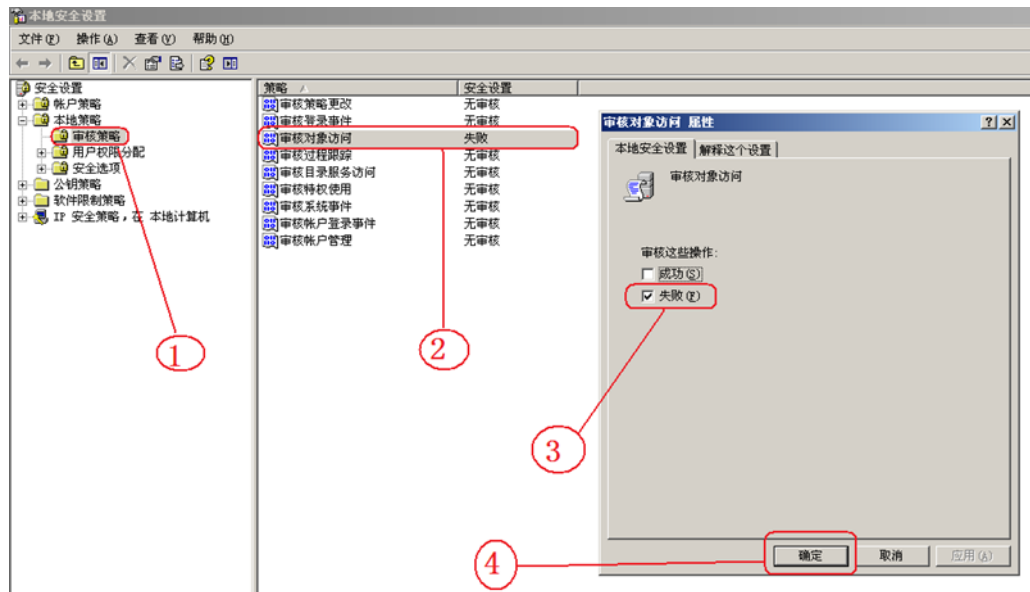
1：依次打開”控制台” -> ”管理工具” -> ”本地安全性原則” -> ”本地策略” -> ”稽核原則” ；

2：按兩下”審核對象訪問” ；

3：彈出的對話方塊中,單選”失敗（F）”這項；

4：確定；

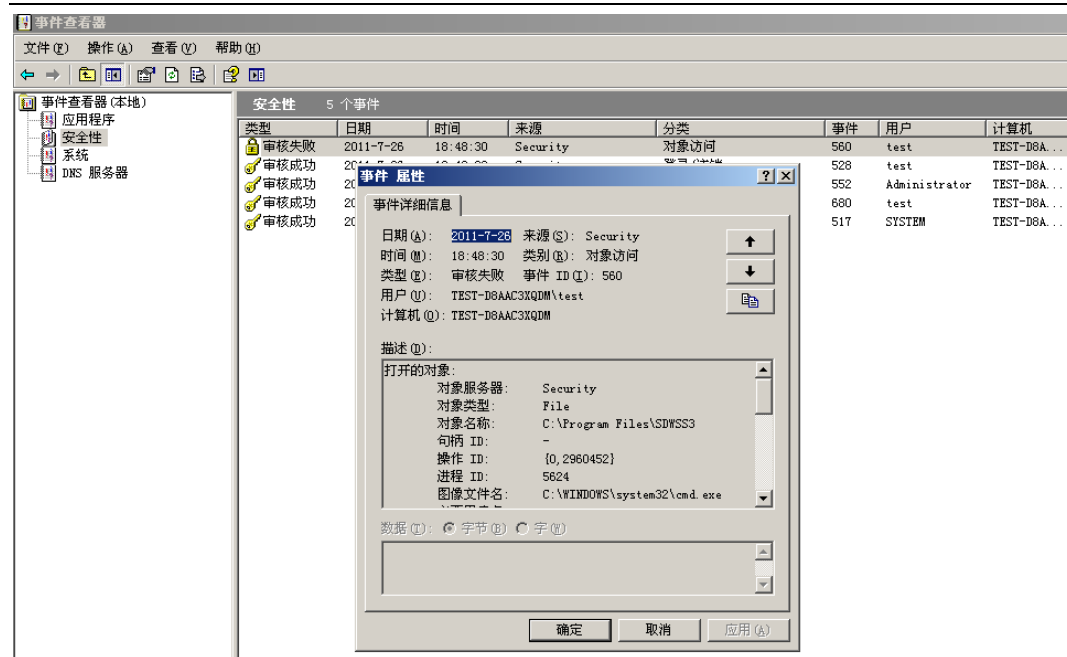
具體示例如下圖：



配置完成後,如果有非管理員使用者訪問產品安裝目錄,不但會被拒絕,而且會產生一條系統安全審計日誌。

二、 查看物件訪問審計日誌

管理員可以通過打開”事件檢視器”中的”安全性”查看到物件訪問審計日誌,如下圖所示：



該日誌說明：2011 年 7 月 26 日,18 點 48 分 30 秒,一個叫 **test** 的非管理員使用者試圖訪問產品安裝目錄” C:\Program Files\SDWSS3” ,被系統阻止,且產生了該條日誌.

第十二章 卸載產品

一、 卸載前的注意事項

- 1.在卸載開始之前,請確認 **IIS** 已經停止運行(在卸載程式的介面中提供了停止和開啟 **IIS** 的按鈕;
- 2.在卸載開始之前,請確認公共策略和所有私有策略中的 **IIS** 配置保護已關閉或取消;

二、 打開卸載程式

點擊”控制台”→”添加或刪除程式”→”深空 web 應用防火牆系統”
→”卸載深空”

三、 開始卸載

在彈出的對話方塊中,按一下”開始卸載(Uninstall)”,卸載過程中程式會提示是否完全卸載,即“刪除所有配置”,如果選擇“保留配置資訊”,則配置資訊依然保留在電腦中,下次安裝時可以直接升級安裝即可恢復之前的配置.

卸載完成後按一下”確定”完成卸載.

第十三章 技術支援及聯繫方式

使用者在使用 深空® web 應用防火牆系統 過程中遇到任何技術問題,可以通過下列方式與本產品製造商 福州深空®資訊技術有限公司 (FuZhou SkyDeep Information Technology Co.,Ltd)取得聯繫.

■統一客服熱線:400-0300-630 Tel: 400-0300-630

■傳真: 0591-22856511 Fax: 86-591-22856511

■電子郵件: sales##sky-deep.com (把##替換成@)

■E-Mail: sales##sky-deep.com (Replace ## as @)

■統一客服 QQ: 652500285 QQ: 652500285

■公司網址 : www.sky-deep.com Website: www.sky-deep.com

■郵編: 350002 Zip Code:350002

■公司地址:中國 福建省 福州市 鼓樓區 工業路 611 號 福建高新技術創業園 北區 6 樓 東 4

■Addr:East 4,6th floor,North Area,Main Building,Fujian High-Tech Pioneer Park,No.611 GongYe Road,Gulou District,Fuzhou,Fujian,China